

User Manual

HS1200N – Wireless N Hotspot



Copyright

Copyright© 2013 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless.



Note: This document is subject to change without notice.

Save our environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

This manual covers the following products:

HS1200N - Wireless N Hotspot Kit

DOCUMENT VERSION	DATE
Initial document release	12/8/2013

Table 1 - Document Revision History

Table of contents

Table of contents	3
Overview	5
Introduction	5
Target audience	5
Prerequisites	5
Notation	5
Product introduction	6
Product overview	6
Package contents	6
System concept	7
Hardware overview	8
Wireless N Hotspot	8
Wireless Ticket Generator	10
Printer	12
Hardware Installation	14
Wireless Hotspot	14
Wireless Ticket Generator and Thermal Printer	14
Establishing a wireless connection	14
Getting Started	15
Configuration Steps	15
Basic Setup	17
Setup Wizard	17
Configuring a billing plan	20
Integrating the HS1200N to your existing network	24
Configure the WAN port	24
Limiting WAN bandwidth and enabling WAN connection detection	27
Configuring Zones	28
Configuring the Wireless Network	31
Wireless General Settings	31
Zone Wireless Settings	32
Wireless Layer 2 firewall	35
Generic Firewall Rules	35
Predefined and Custom Service Protocols	38
Advanced	40
Configuring network access	41
Type of Users	41
Local	41
RADIUS	44
On-Demand User	47
Free Authentication	54
User Login	55
Default Authentication	55
Login with Suffix	55
Banning Users	57
Black List	57
Group	58
Policy	58
Schedule	59
Firewall	60
QoS Profile	62
Routing	63
User Privilege	64
Accessing the Network without Authentication	65
DMZ	65
Virtual Server	66
Privilege List	67
Privilege IP	67
Privilege MAC	68
Privilege IPv6	68
Disable Authentication in Public Zone	69
User Login and Logout	70
Before Login	70
Internal Domain Name with Certificate	71
Walled Garden	72
Walled Garden AD	73
After Login	74

Idle Timer	74
Multiple Login	75
Networking Features of a Gateway	75
Port and IP Forwarding	76
System Management and Utilities	77
System Time	77
Management IP Address List	78
IP Address for Accessing User Log	79
SNMP	80
Administration	81
Changing Admin Passwords	84
Backup / Restore and Reset to the Factory Default	85
Firmware Upgrade	86
Restart	86
Network Utility	87
Wake-on-LAN	87
Ping	87
Trace Route	87
Show ARP Table	87
Monitor IP Link	88
Console Interface	88
System Status and Reports	90
Viewing the Status	90
System Status	90
Interface Status	92
Routing Table	96
Current Users	97
Session List	98
User Log	98
Local User Monthly Network Usage Report	100
System Related Logs	101
DHCP Lease	101
Notification	102
E-Mail	103
SYSLOG	104
FTP	104
Advanced Applications	106
Upload/Download Local User Accounts	106
RADIUS Advanced Settings	108
Roaming Out	109
Customizable Pages	110
Appendix A: Policy Priority	111
Global Policy, Authentication Policy and User Policy	111
Appendix B: WDS Management	112
Appendix C: RADIUS Accounting	113
Description	113
VSA configuration in RADIUS server (IAS Server)	114
VSA configuration in RADIUS server (FreeRADIUS)	117
Appendix D: On-demand Account types & Billing Plan	120
External Payment Gateways	129
Payments via Authorize.Net	129
Payments via PayPal	132
Payments via SecurePay	134
Payments via World Pay	136
Appendix F: Portal Page Customization	139
How External Pages Operate	139
URL Variables from Gateway	142
URL Variables to Gateway	145

Overview

Introduction

This document provides you all the information you need to set up, configure and use the Wireless N Hotspot.

Target audience

This manual is for wireless service providers or network administrators to set up a network environment using the HS1200N system. It contains step-by-step procedures and graphic examples to guide IT staff or individuals with some network system knowledge to complete the installation.

Prerequisites

Before continuing with the installation of your Wireless N Hotspot, please confirm that you have the following:

-  A device with a working Ethernet network adapter.
-  A web browser such as Internet Explorer, Mozilla Firefox or Google Chrome.

Notation

The following symbols are used in this user guide:



The following note requires attention.



The following note provides a warning.



The following note provides useful information.

Product introduction

Product overview

The HS1200N is an economical and feature rich Wireless Hotspot Gateway. Feature-packed for hotspot operation, the HS1200N comes with a built-in wireless 802.11 n/b/g MIMO access point, web server and web pages for client log in, simple user/visitor account management tool, payment plans, multiple credit card payment options, traffic logs, and IP sharing. The HS1200N also includes the extra advantage of being wall-mountable and dust-proof with an IP50 metal housing.

Package contents

The Wireless N Hotspot package includes:

-  1 x HS1200N Wireless Hotspot Gateway
-  1 x Quick start guide
-  1 x Console cable
-  1 x Ethernet cable
-  1 x 5V DC Power adapter
-  2 x WiFi antennas

The Wireless Ticket Generator and Printer package includes:

-  1 x Wireless Ticket Generator
-  1 x Printer
-  1 x DB9 Adapter cable
-  1 x Printer thermal paper roll
-  1 x 8.4VDC/3A Power adapter (for Printer)
-  1 x 5V/3A DC Power adapter (for Wireless Ticket Generator)
-  1 x WiFi antenna (for Wireless Ticket Generator)

If any of these items are missing or damaged, please contact NetComm Wireless Support immediately. The NetComm Wireless Support website can be found at: <http://support.netcommwireless.com>.

We recommend that you keep the original packaging materials in case repair or maintenance is necessary. This will protect the HS1200N from damage during transport.

System concept

The HS1200N is capable of managing user authentication, authorisation and accounting. The user account information is stored in the local database or a specified external RADIUS database server. Featuring user authentication and integrated with an external payment gateway, the HS1200N allows users to easily pay the designated fee using credit cards through a variety of payment gateways including Authorize.Net, PayPal, SecurePay, and WorldPay to gain access to your Internet service.

The HS1200N introduces the concept of Zones – a Private Zone and Public Zone, each with its own definable access control profiles. Clients in the Private Zone are not required to be authenticated before using the network services while clients in the Public Zone must be authenticated before using the network services. This enables hotspot owners to deploy wireless network services for clients and then manage the network as well. The following diagram illustrates how the HS1200N package is typically deployed to manage the Internet and access to network services.

Hardware overview

Wireless N Hotspot

Front Panel



NUMBER	BUTTON	DESCRIPTION
1	Quick button	Press this button to quick print an account generated from billing plan 1.
2	WES button	Press and hold over 5 seconds to initiate Master Mode for the WES process. Press and release to initiate Slave Mode for the WES process.

NUMBER	LED	DESCRIPTION		
3	Power	When illuminated, the device is on and correctly powered.		
4	Status	When illuminated, the system is ready.		
5	Wireless	When illuminated, this wireless LED indicates that the network interface is ready for service.		
6	WAN	Illuminates in orange to indicate that the WAN port is connected to a 1000Mbps link		
		Illuminates in green to indicate that the WAN port is connected to a 10/100Mbps link		
7	LAN1 – LAN4	Illuminates in orange to indicate that the LAN port is connected to a 1000Mbps connection.		
		Illuminates in green to indicate that the LAN port is connected to a 10/100Mbps connection.		
8	USB	Reserved for future use.		
9	WES		MASTER	SLAVE
		WES Start	LED Blinks Slowly (Green)	LED Blinks Slowly (Red)
		WES Negotiate	Blinking normally (Green)	Blinking normally (Red)
		WES Timeout	LED On (Green)	LED On (Red)
		WES Success	LED On (Red)	LED On (Green)
		WES Fail	LED On (Green)	LED On (Red)

Rear Panel



NUMBER	INTERFACE	DESCRIPTION
1	Antenna Connector	Attach the included WiFi antennas here. (The HS1200N offers 1 WiFi interface with 2 SMA connectors)
2	WAN	For connecting wired external network.
3	LAN 1-4	For connecting to a wired internal network. LAN 1 and LAN 2 are mapped to the "Private Zone" by default LAN 3 and LAN 4 are mapped to the "Public Zone" by default.
4	USB 2.0	Reserved for future use.
5	Console	For connecting an RS-232 console cable to perform system management.
6	Power Jack (5V /3A)	For connecting to the provided external power supply.
7	Restart / Reset	Press once to restart the system. Press and hold for more than 5 seconds to reset to factory default settings.

Wireless Ticket Generator

Keypad Panel



NUMBER	INTERFACE	DESCRIPTION
1	Keypad	Used for entering a profile number to send to the printer for ticket generation.
2	Status LEDs	Displays indicators for Power, Ready Status, Ethernet and WLAN.

Left Panel



NUMBER	INTERFACE	DESCRIPTION
3	Restart / Reset button	Press the button to restart the ticket generator. Hold for 5 seconds and then release to restore to factory default settings.
4	TAS button	Terminal Auto Setup (TAS). Hold for 3 seconds and then release to initiate the auto uplink connection process.

Right Panel



NUMBER	INTERFACE	DESCRIPTION
5	Console port	Serial port for connection to the thermal printer.
6	Ethernet port	RJ-45 Ethernet port for connection to the Wireless N Hotspot.
7	Power jack	Connect the supplied 5V / 3.0A power supply
8	WiFi antenna connector	Attach the supplied WiFi antenna here by screwing it on in a clockwise direction.

Printer

Top Panel



NUMBER	INTERFACE	DESCRIPTION
1	Power LED	When the printer is correctly connected to a power source, this LED illuminates in blue.
2	Error LED	This illuminates in red when the printer has encountered an error, such as a paper jam.
3	Paper LED	This illuminates in red when the printer has run out of paper or printer cover is not closed properly.
4	Feed button	Use the feed button to feed the thermal paper from the printer.

Rear Panel



NUMBER	INTERFACE	DESCRIPTION
1	RJ-11 port	RJ11 port for connection to the Cash Drawer
2	Console port	Serial port for connection to the wireless key generator.
3	Power jack	Connect the provided 8.4V / 3.0A power supply to the power jack.
4	Power switch	Used to turn the printer on and off.

Hardware Installation

Wireless Hotspot

Please follow the steps below to install the HS1200N Wireless N Hotspot.

1. Place the HS1200N in the location that provides the best possible signal.

The best location for the HS1200N is usually at the centre of your wireless network. This ensures it is able to get a clear wireless signal.

2. Connect the HS1200N to your outbound network device.

Connect one end of the supplied Ethernet cable to the WAN port on the front of the HS1200N. Connect the other end of the Ethernet cable to the device in use that will be used to provide access to the Internet. This may be an ADSL Router, a cable modem or a switch/hub. The WAN LED illuminates to indicate a proper connection.

3. Connect the HS1200N to your local area network device.

Connect one end of an Ethernet cable to the LAN1 port on the front of the HS1200N. Connect the other end of the cable to the Ethernet port on the computer being used to configure the HS1200N. The LAN1 LED illuminates to indicate a proper connection has been made.

Note: The HS1200N has two virtual 'zones' (Private and Public). These zones are mapped to LAN1 (192.168.110.1) and LAN2 (192.168.120.1) respectively.

4. Connect the power supply to the HS1200N.

Connect the DC power adapter to the power socket on the rear panel of the HS1200N. Wait up to 10 minutes for the router to start up.

Note:

-  Only use the power adapter supplied with the HS1200N. Using a different power adapter may damage the system.
-  To verify the wired connection between the HS1200N and the switch/hub/router, you can also check the LED status indicators of these network devices.

Wireless Ticket Generator and Thermal Printer

Please follow the steps below to install the Wireless Ticket Generator and Thermal Printer.

1. Place the Wireless Ticket Generator and Thermal Printer close to one another and in the position you would like to use them.
2. Attach the included WiFi antenna to the WiFi antenna connector on the Wireless Ticket Generator by turning it clockwise.
3. Connect the smaller end of the included console cable to the console port of the Wireless Ticket Generator and connect the larger end to the console port on the rear panel of the Thermal Printer. Tighten the shoulder screws on both ends of the console cable to prevent accidental disconnection.
4. Connect the supplied 5V / 3.0A power supply to the power jack on the right side panel of the Wireless Ticket Generator.
5. Connect the supplied 8.4V / 3.0A power supply to the power jack on the rear panel of the Thermal Printer. Use the power switch on the rear panel of the Thermal Printer to turn it on.

Establishing a wireless connection

The Wireless Ticket Generator must establish a secure connection with the Wireless N Hotspot in order to create user accounts and send this information to the Thermal Printer. To establish a secure connection, on the Wireless Ticket Generator, press and hold the TAS button on the left panel for 3 seconds and then release it. The Wireless Ticket Generator searches for the Wireless N Hotspot and creates a secure connection between them. This process takes about 30 seconds.

The hardware setup is now complete.

Getting Started

The HS1200N offers a web based configuration page. After completing the hardware installation above, the HS1200N can be configured through a computer using a web browser with JavaScript enabled.

The default LAN IP addresses are:

LAN1 and LAN2: 192.168.110.1 – These are mapped to the Private Zone; user authentication is not required to access network resources.

LAN3 and LAN4: 192.168.120.1 – These are mapped to the Public Zone; user authentication is required to access network resources.

Note: The following instructions use the administration computer connected to the LAN1 port.

Configuration Steps

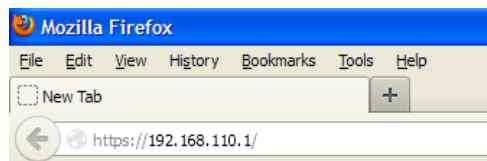
Once the hardware installation steps are complete, set your computer to “Obtain an IP address automatically” in the TCP/IP settings when logged in to the PC as an administrator. If you have not modified your TCP/IP settings, it should already be configured in this way.

Connect one end of the provided Ethernet cable to the PC and the other end to LAN port 1.

Open a web browser and type <https://192.168.110.1> or <http://192.168.110.1> in the address field and press **Enter**.



Note: Use “https” for a secure connection.



For the first time, if the HS1200N is not using a **trusted SSL certificate**, there will be a “**Certificate Error**”. This is because the browser treats the HS1200N as an untrusted website. Please press “**Continue to this website**” to continue.



If you are unable to see the login screen verify your computer is configured to obtain an IP address automatically. You can also try using a static IP address such as 192.168.110.xxx (where xxx is a number between 2 and 254) and then try loading the page again. For assistance configuring your computer, please refer to Appendix A: Network Configuration on a Computer.

The following login page appears. Enter **admin** in both the username and password fields then click the **Login** button to continue.



The main configuration screen appears after successfully logging in.



Basic Setup

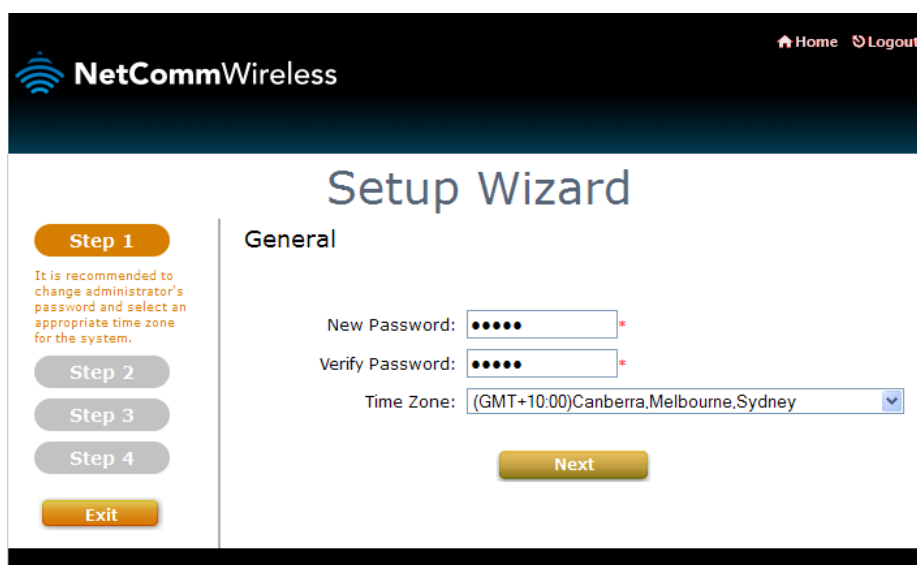
Setup Wizard

The HS1200N provides a setup wizard for quick and easy configuration. Click on the Setup Wizard button to start the configuration process.



Step 1: General

Step 1 of the setup wizard enables you to configure your Administrator password, System Time settings and the web page address to which connected computers are redirected.

A screenshot of the NetCommWireless Setup Wizard, Step 1: General. The header shows the NetCommWireless logo and 'Home' and 'Logout' links. The main heading is 'Setup Wizard'. On the left, there is a sidebar with 'Step 1' highlighted, and buttons for 'Step 2', 'Step 3', 'Step 4', and 'Exit'. A note in the sidebar states: 'It is recommended to change administrator's password and select an appropriate time zone for the system.' The main content area is titled 'General' and contains three fields: 'New Password' (with a password mask), 'Verify Password' (with a password mask), and 'Time Zone' (a dropdown menu showing '(GMT+10:00)Canberra,Melbourne,Sydney'). A 'Next' button is located at the bottom right of the form.

Enter a new administrator password in the **New Password** field and then re-enter the same new password in the **Verify Password** field.



Note: A maximum of 20 characters (with no spaces) is allowed. For security purposes, we strongly recommended that you change the administrator password from the default setting.

Select the appropriate time zone from the **Time Zone** drop-down list.

Click the **Next** button to continue.

Step 2: WAN and Wireless Interfaces

Step 2 of the setup wizard configures your WAN and Wireless network settings.

Select the type of interface for the WAN connection.

Static: Enter the appropriate IP address, subnet mask, default gateway and DNS server information for your WAN device (such as an ADSL modem or 3G router).

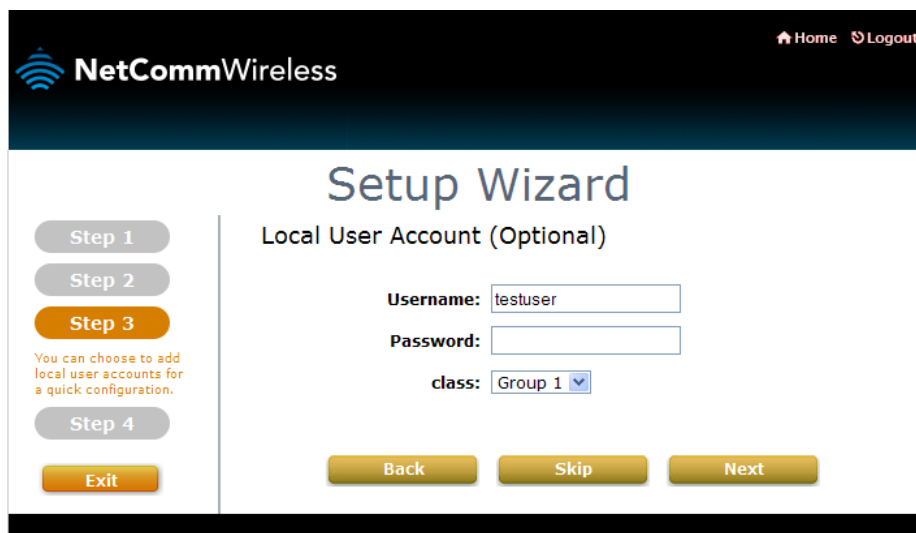
Dynamic: Network configuration information is automatically obtained via DHCP from your WAN device (such as an ADSL modem or 3G router).

PPPoE: Enter the username and password required to connect to your WAN service.

Step 3: Add a Local User Account (Optional)

Step 3 is optional and allows you to quickly create a local user account which has internet access. If you do not wish to do this, click the **Skip** button.

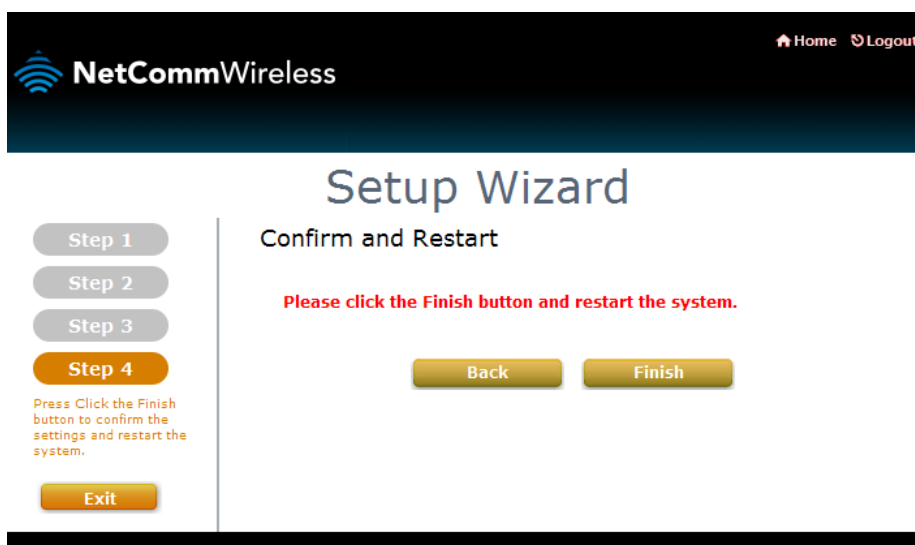
Enter a username and password and use the **class** drop down list to select a group to which the user belongs. The class is used to define the policy for the account. Refer to the user guide for more information on groups and how to log in with a local user account. When you have entered the details of the account, click the **Next** button.



The screenshot shows the 'Setup Wizard' interface for 'Local User Account (Optional)'. On the left, a sidebar contains buttons for Step 1, Step 2, Step 3 (highlighted in orange), Step 4, and Exit. Below Step 3, a note says: 'You can choose to add local user accounts for a quick configuration.' The main area has input fields for 'Username:' (containing 'testuser'), 'Password:', and a 'class:' dropdown menu (set to 'Group 1'). At the bottom are 'Back', 'Skip', and 'Next' buttons. The top header includes the NetComm Wireless logo and 'Home' and 'Logout' links.

Step 4: Confirm and Restart

Step 4 asks you to confirm your settings. If you need to make changes, click the **Back** button until you get to the screen on which you need to make changes. Otherwise, click the **Finish** button.



The screenshot shows the 'Setup Wizard' interface for 'Confirm and Restart'. On the left, a sidebar contains buttons for Step 1, Step 2, Step 3, Step 4 (highlighted in orange), and Exit. Below Step 4, a note says: 'Press Click the Finish button to confirm the settings and restart the system.' The main area displays the text 'Please click the Finish button and restart the system.' in red. At the bottom are 'Back' and 'Finish' buttons. The top header includes the NetComm Wireless logo and 'Home' and 'Logout' links.

You are prompted to confirm the restart of the system.

Are you sure to restart the system?

Click **OK**. The Wireless N Hotspot reboots and the following screen is displayed.

 **NetCommWireless** Home Logout

Setup Wizard

Confirm and Restart

.....

Step 1

Step 2

Step 3

Step 4

Press Click the Finish button to confirm the settings and restart the system.

Exit



Note: The Wireless N Hotspot must be restarted for the configuration to take effect. The restart process can take up to 10 minutes to complete.

When the login page is displayed, the Wireless N Hotspot has finished rebooting.

 **NetCommWireless**



Username:

Password:

[Change password?](#)

Login

Configuring a billing plan

A billing plan is a profile which you configure on the hotspot for use with the Wireless Ticket Generator. Billing plans can be created based on usage time or usage volume.

This guide demonstrates how to configure a simple billing plan providing one hour of internet access.

Log in to the wireless hotspot as described on page 8 of this quick start guide.

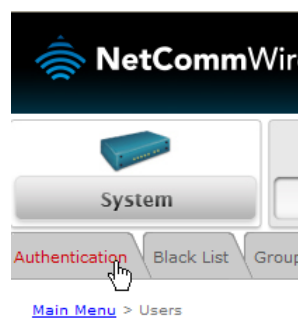
1. Click on the **Main Menu** button.



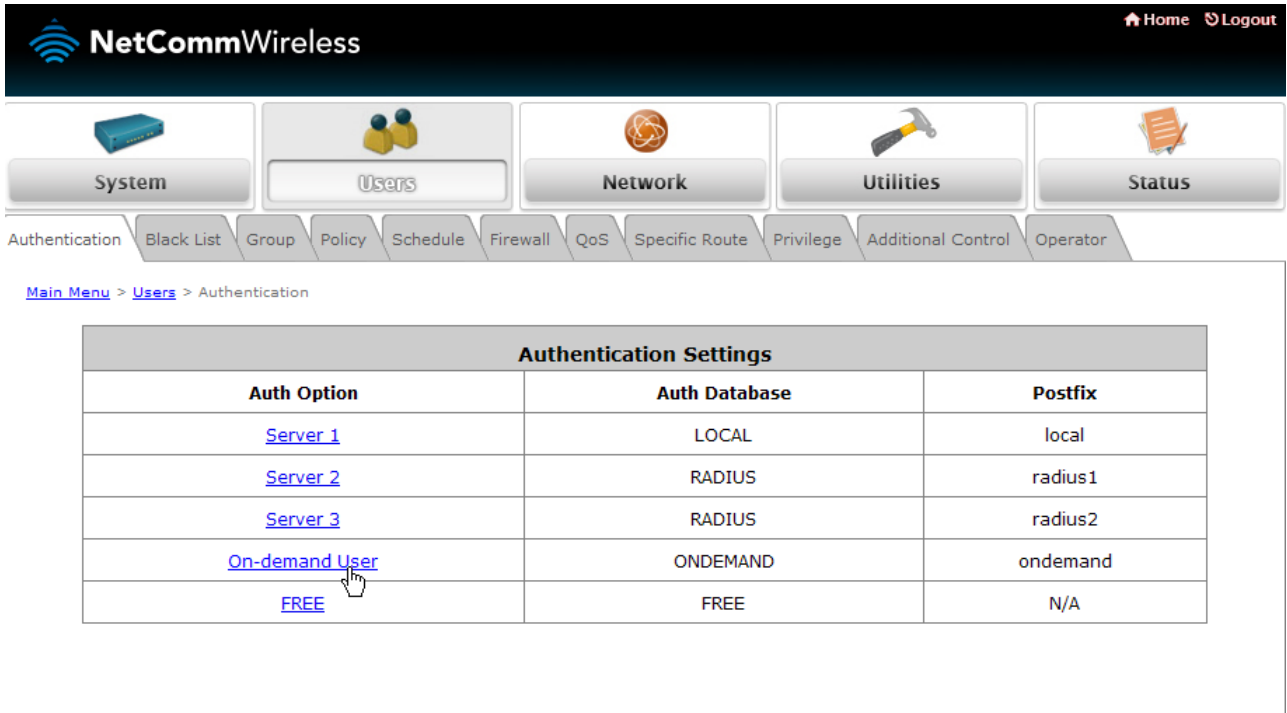
2. Click on the **Users** menu.



3. Click on the **Authentication** tab.



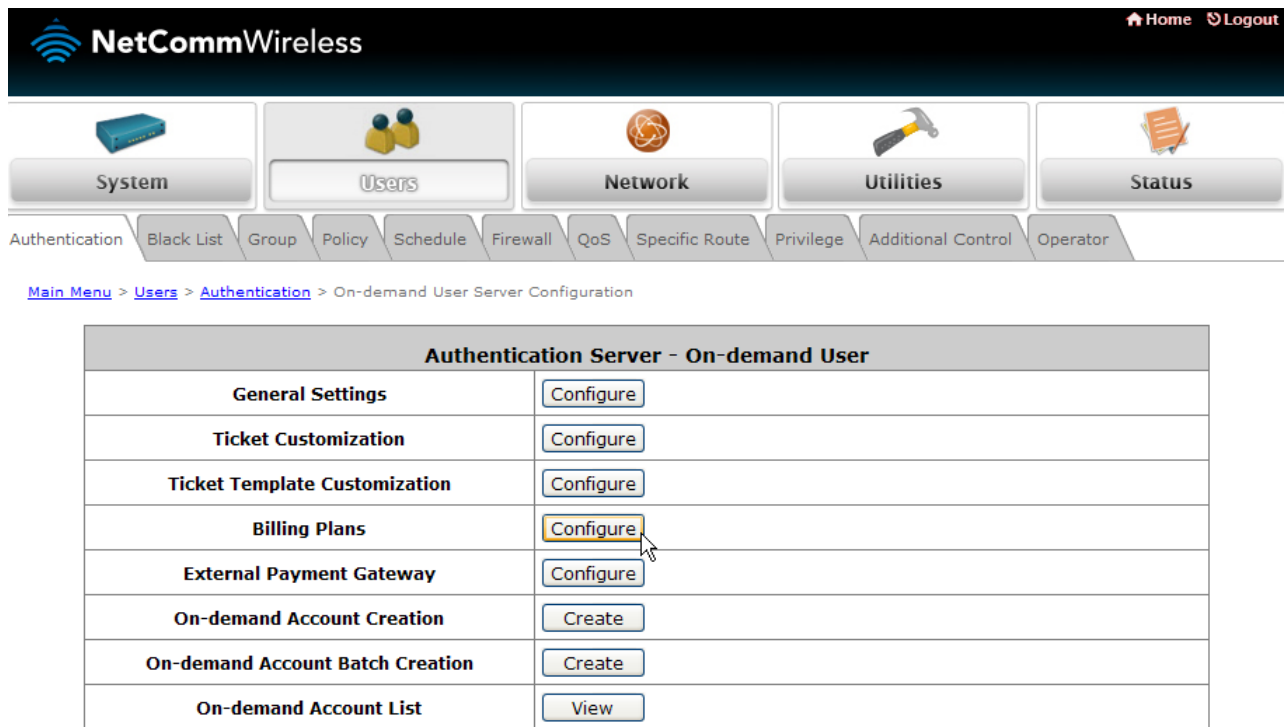
4. Select the **On-demand User** link.



The screenshot shows the NetCommWireless web interface. The top navigation bar includes 'Home' and 'Logout' links. Below the main menu, the 'Users' tab is selected. The 'Authentication' sub-tab is active, displaying a table titled 'Authentication Settings'.

Auth Option	Auth Database	Postfix
Server 1	LOCAL	local
Server 2	RADIUS	radius1
Server 3	RADIUS	radius2
On-demand User	ONDEMAND	ondemand
FREE	FREE	N/A

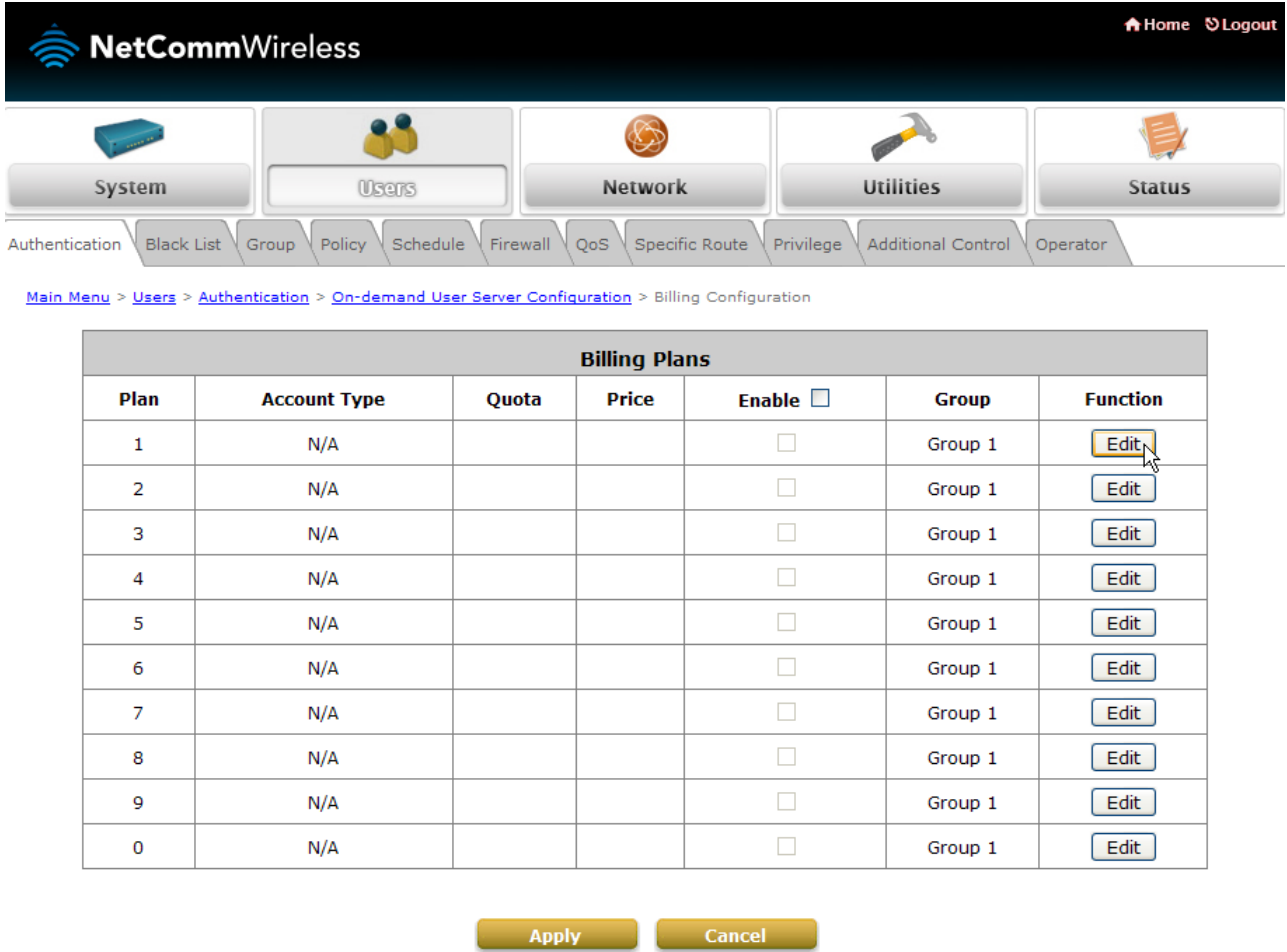
5. Next to **Billing Plans**, click the **Configure** button.



The screenshot shows the NetCommWireless web interface. The top navigation bar includes 'Home' and 'Logout' links. Below the main menu, the 'Users' tab is selected. The 'Authentication' sub-tab is active, displaying a table titled 'Authentication Server - On-demand User'.

Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Ticket Template Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account Batch Creation	Create
On-demand Account List	View

6. Next to plan number 1, click the **Edit** button.

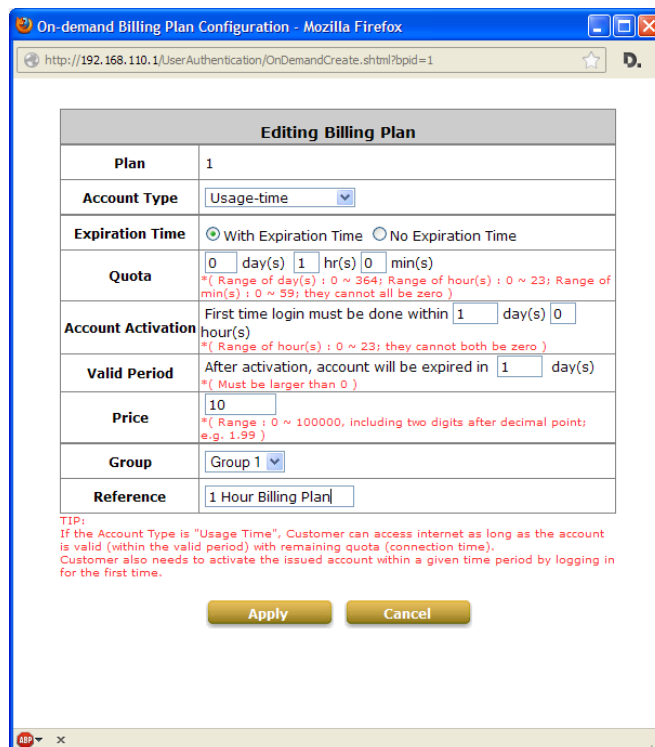


Billing Plans

Plan	Account Type	Quota	Price	Enable ☐	Group	Function
1	N/A			☐	Group 1	Edit
2	N/A			☐	Group 1	Edit
3	N/A			☐	Group 1	Edit
4	N/A			☐	Group 1	Edit
5	N/A			☐	Group 1	Edit
6	N/A			☐	Group 1	Edit
7	N/A			☐	Group 1	Edit
8	N/A			☐	Group 1	Edit
9	N/A			☐	Group 1	Edit
0	N/A			☐	Group 1	Edit

Apply **Cancel**

7. Enter the desired settings into the pop-up window that appears.



On-demand Billing Plan Configuration - Mozilla Firefox

http://192.168.110.1/UserAuthentication/OnDemandCreate.shtml?bpid=1

Editing Billing Plan

Plan	1
Account Type	Usage-time
Expiration Time	☒ With Expiration Time ☐ No Expiration Time
Quota	0 day(s) 1 hr(s) 0 min(s) *(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Account Activation	First time login must be done within 1 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 1 day(s) *(Must be larger than 0)
Price	10 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	1 Hour Billing Plan

TIP:
If the Account Type is "Usage Time", Customer can access internet as long as the account is valid (within the valid period) with remaining quota (connection time).
Customer also needs to activate the issued account within a given time period by logging in for the first time.

Apply **Cancel**

This example shows you how to configure a billing plan for one hour of access:

8. From the **Account Type** drop down list, select **Usage-time**.
 9. Select the **With Expiration Time** option.
 10. Set **Quota** to **0** day(s) **1** hr(s) and **0** min(s).
 11. Set **Account Activation** to **1** day(s) **0** hour(s). This means the account must be used within 1 day or it will become inactive.
 12. Set **Valid Period** to 1 day(s). This means that after the account has been activated, it will expire in 1 day.
 13. Set **Price** to whatever you wish to charge the customer for 1 hour of internet access. In this example we are charging 10 dollars.
 14. Use the **Group** drop down menu to assign a Group for the billing plan.
 15. If you want to add some notes to the billing plan for your own reference, such as a name for it, enter it into the **Reference** field.
- Click the **Apply** button. You may now generate a ticket using the Wireless Ticket Generator by pressing number **1** and pressing **ENTER** on the Wireless Ticket Generator keypad.

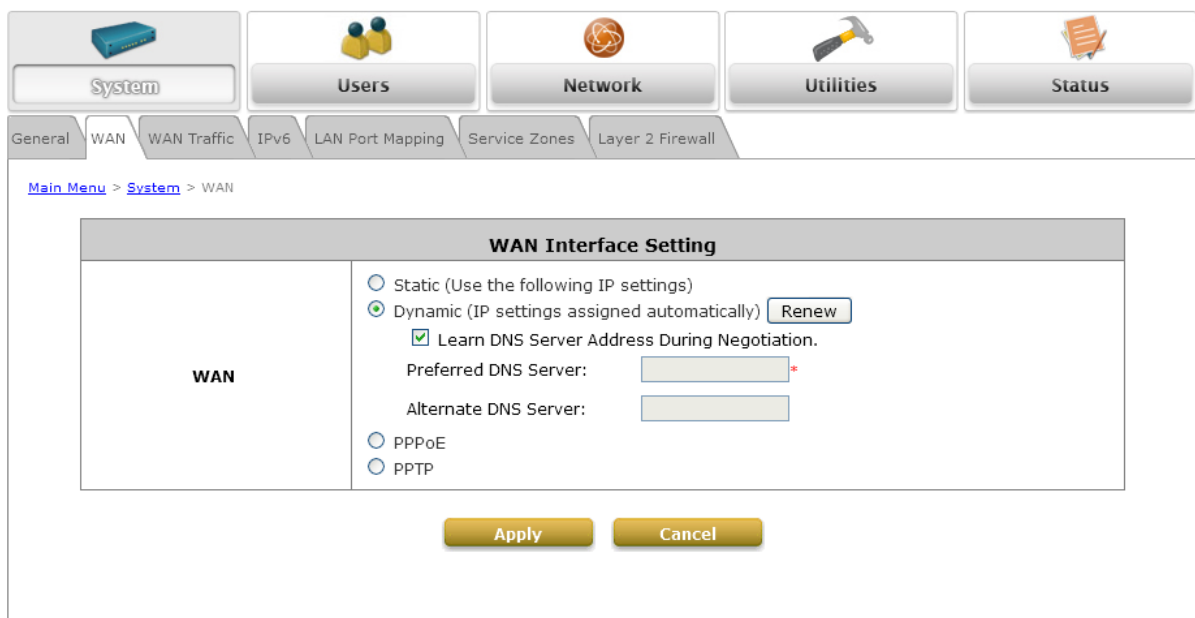
Integrating the HS1200N to your existing network

In a typical network environment, the main role of the HS1200N is to manage network access from the internal network to the Internet. Thus, the first step is to prepare an Internet connection from your ISP (Internet Service Provider) and connect it to the WAN port of The HS1200N.

Configure the WAN port

There are 4 connection types for the WAN Port: **Static**, **Dynamic**, **PPPoE** and **PPTP**.

To configure the WAN port, go to **System >> WAN**.



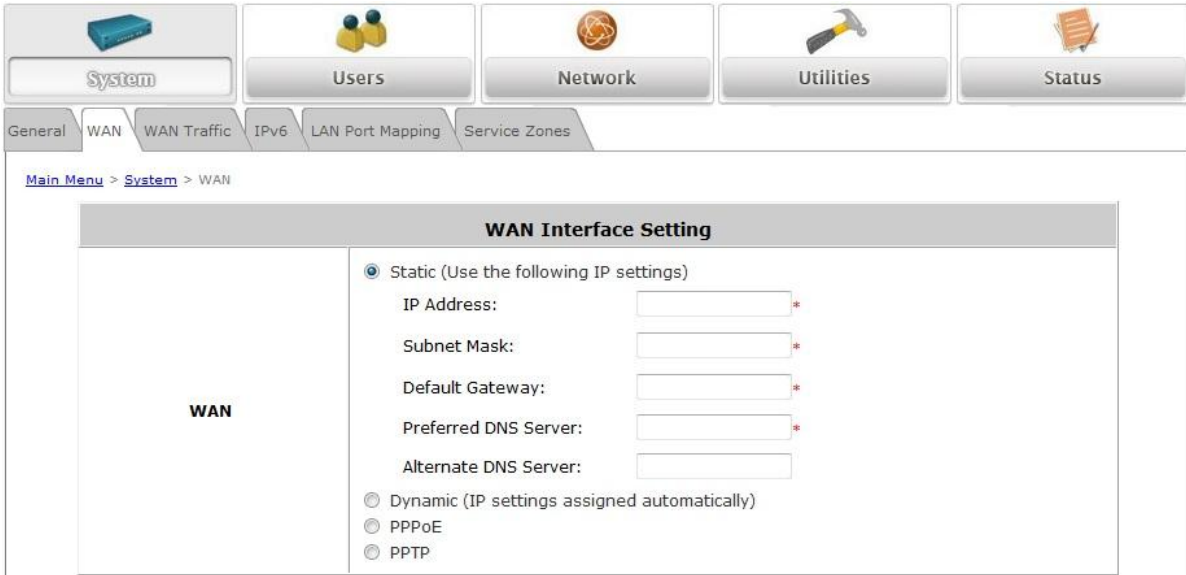
The screenshot displays the configuration interface of the NetComm Wireless HS1200N. At the top, there are five main menu buttons: System, Users, Network, Utilities, and Status. Below these, a series of sub-menu tabs are visible: General, WAN, WAN Traffic, IPv6, LAN Port Mapping, Service Zones, and Layer 2 Firewall. The 'WAN' tab is currently selected. The main content area shows the 'WAN Interface Setting' page. On the left, there is a label 'WAN'. On the right, there are four radio button options for connection types: Static (Use the following IP settings), Dynamic (IP settings assigned automatically), PPPoE, and PPTP. The 'Dynamic' option is selected. A 'Renew' button is located next to the 'Dynamic' option. Below the radio buttons, there is a checkbox labeled 'Learn DNS Server Address During Negotiation' which is checked. Underneath this checkbox, there are two text input fields: 'Preferred DNS Server:' and 'Alternate DNS Server:'. The 'Preferred DNS Server' field has a red asterisk next to it. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

The parameters related to each connection method are described on the following pages.

Static IP

Use this method if you wish to manually specify the IP address of the WAN port. The fields with red asterisks are mandatory.

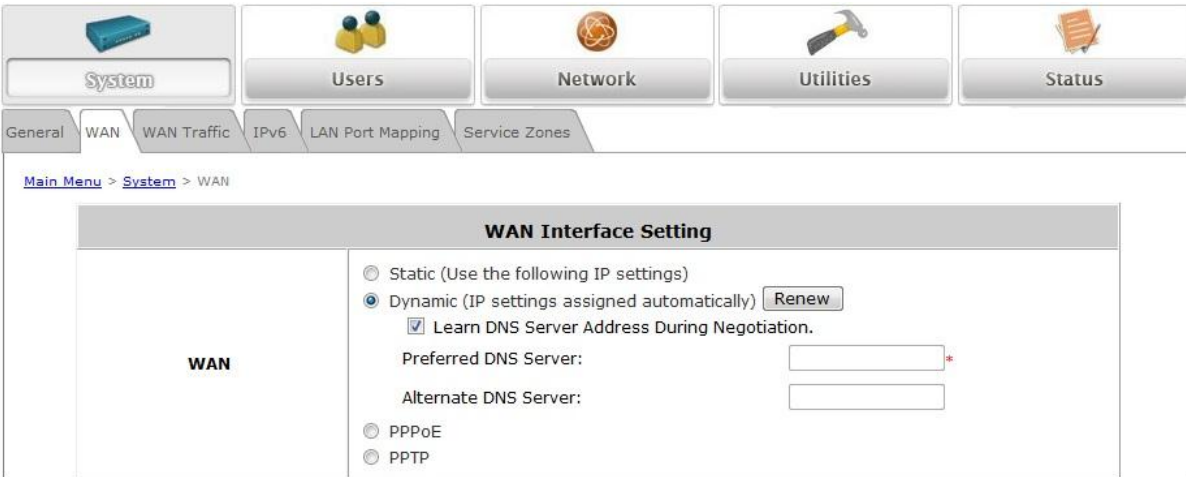
-  **IP Address:** The IP address of the WAN port.
-  **Subnet Mask:** The subnet mask of the WAN port.
-  **Default Gateway:** The gateway of the WAN port.
-  **Preferred DNS Server:** The primary DNS Server of the system.
-  **Alternate DNS Server:** The substitute DNS Server of the system. This is an optional field.



The screenshot shows the 'System' tab selected in the top navigation bar. Below it, the 'WAN' sub-tab is active. The 'WAN Interface Setting' section is displayed, showing the 'Static (Use the following IP settings)' option selected. The fields for IP Address, Subnet Mask, Default Gateway, Preferred DNS Server, and Alternate DNS Server are all empty and marked with a red asterisk (*). Below these fields, the 'Dynamic (IP settings assigned automatically)' option is also visible, along with 'PPPoE' and 'PPTP' options.

Dynamic

Select Dynamic IP when you have the gateway connected to a network where there is a DHCP server available. Click the **Renew** button to get an IP address automatically.

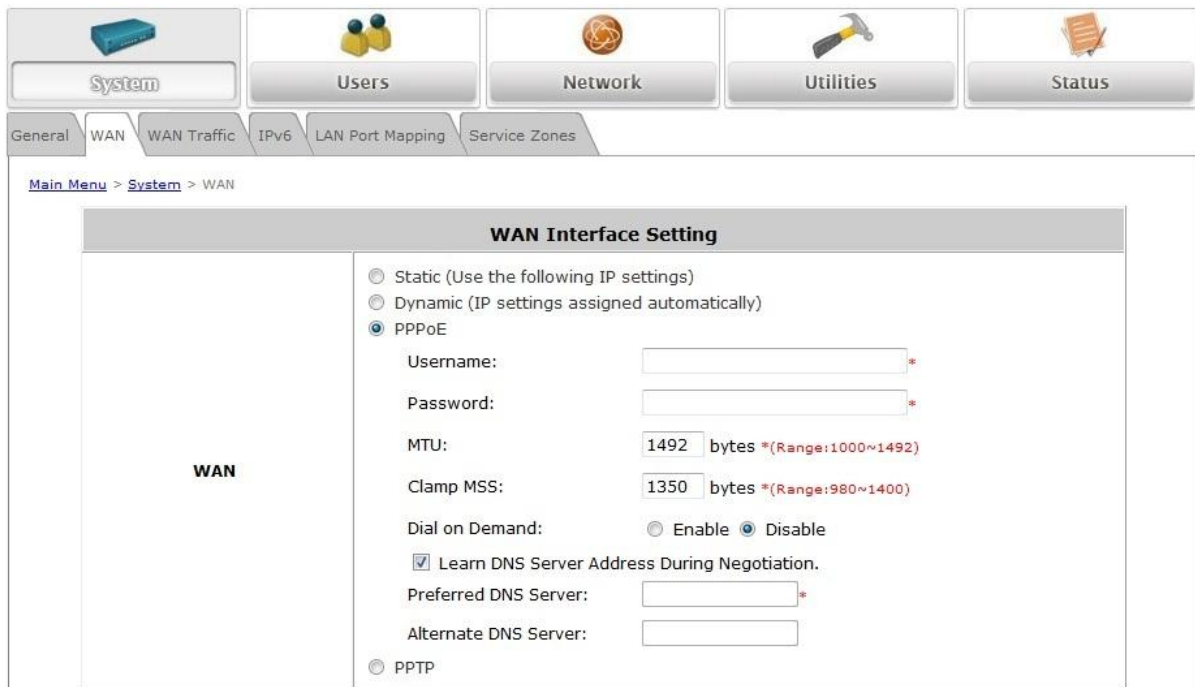


The screenshot shows the 'System' tab selected in the top navigation bar. Below it, the 'WAN' sub-tab is active. The 'WAN Interface Setting' section is displayed, showing the 'Dynamic (IP settings assigned automatically)' option selected. A 'Renew' button is visible next to the 'Dynamic' option. The 'Learn DNS Server Address During Negotiation' checkbox is checked. The fields for Preferred DNS Server and Alternate DNS Server are empty and marked with a red asterisk (*). Below these fields, the 'PPPoE' and 'PPTP' options are also visible.

PPPoE

Select PPPoE if you wish to have your gateway manage the status of the internet connection. Set the “Username”, “Password”, “MTU” and “Clamp MSS” fields.

When Dial-on-Demand is enabled, the gateway automatically disconnects the internet connection when the configured **Maximum Idle Time** is reached.

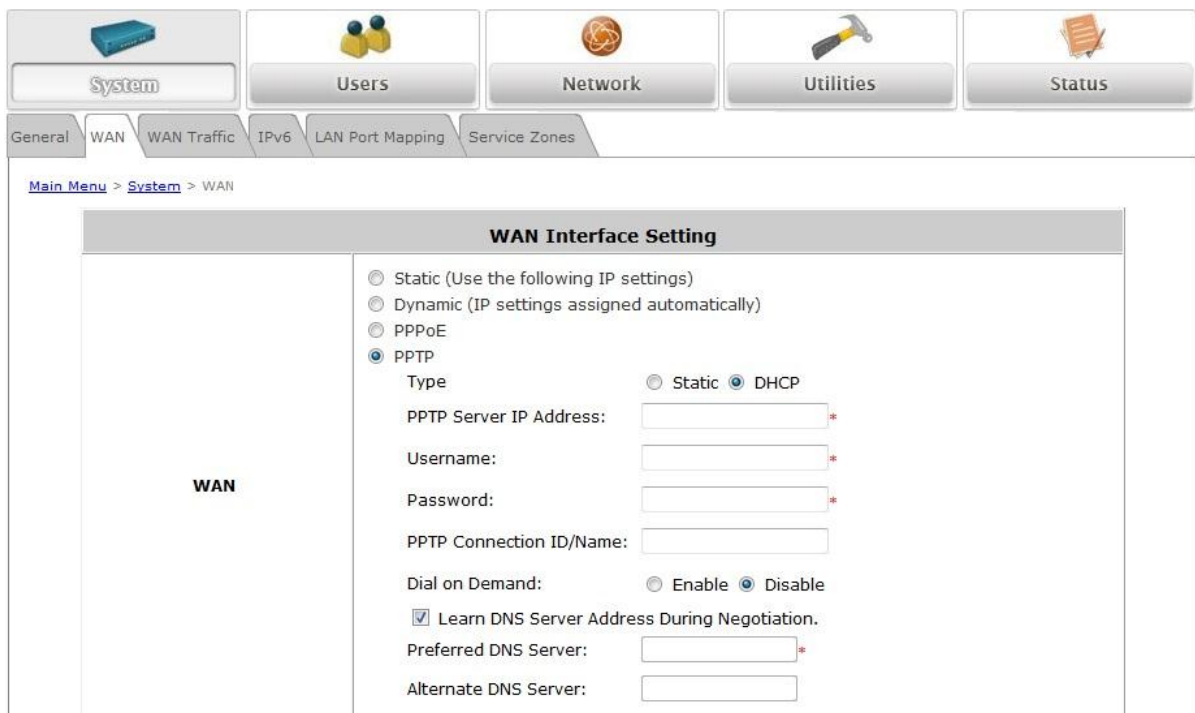


The screenshot shows the NetComm Wireless web interface. At the top, there are five main tabs: System, Users, Network, Utilities, and Status. Below these, there are sub-tabs for General, WAN, WAN Traffic, IPv6, LAN Port Mapping, and Service Zones. The 'WAN' sub-tab is selected. The main content area is titled 'WAN Interface Setting'. On the left, there is a 'WAN' label. On the right, there are several configuration options:

- ☐ Static (Use the following IP settings)
- ☐ Dynamic (IP settings assigned automatically)
- ☒ PPPoE
 - Username: *
 - Password: *
 - MTU: bytes *(Range:1000~1492)
 - Clamp MSS: bytes *(Range:980~1400)
 - Dial on Demand: ☐ Enable ☒ Disable
 - ☒ Learn DNS Server Address During Negotiation.
 - Preferred DNS Server: *
 - Alternate DNS Server:
- ☐ PPTP

PPTP

PPTP is a method used to connect the gateways internet connection. If supported by your ISP, you will have been issued with an account with a password as well as the PPTP server address.



The screenshot shows the NetComm Wireless web interface. At the top, there are five main tabs: System, Users, Network, Utilities, and Status. Below these, there are sub-tabs for General, WAN, WAN Traffic, IPv6, LAN Port Mapping, and Service Zones. The 'WAN' sub-tab is selected. The main content area is titled 'WAN Interface Setting'. On the left, there is a 'WAN' label. On the right, there are several configuration options:

- ☐ Static (Use the following IP settings)
- ☐ Dynamic (IP settings assigned automatically)
- ☐ PPPoE
- ☒ PPTP
 - Type: ☐ Static ☒ DHCP
 - PPTP Server IP Address: *
 - Username: *
 - Password: *
 - PPTP Connection ID/Name:
 - Dial on Demand: ☐ Enable ☒ Disable
 - ☒ Learn DNS Server Address During Negotiation.
 - Preferred DNS Server: *
 - Alternate DNS Server:

Limiting WAN bandwidth and enabling WAN connection detection

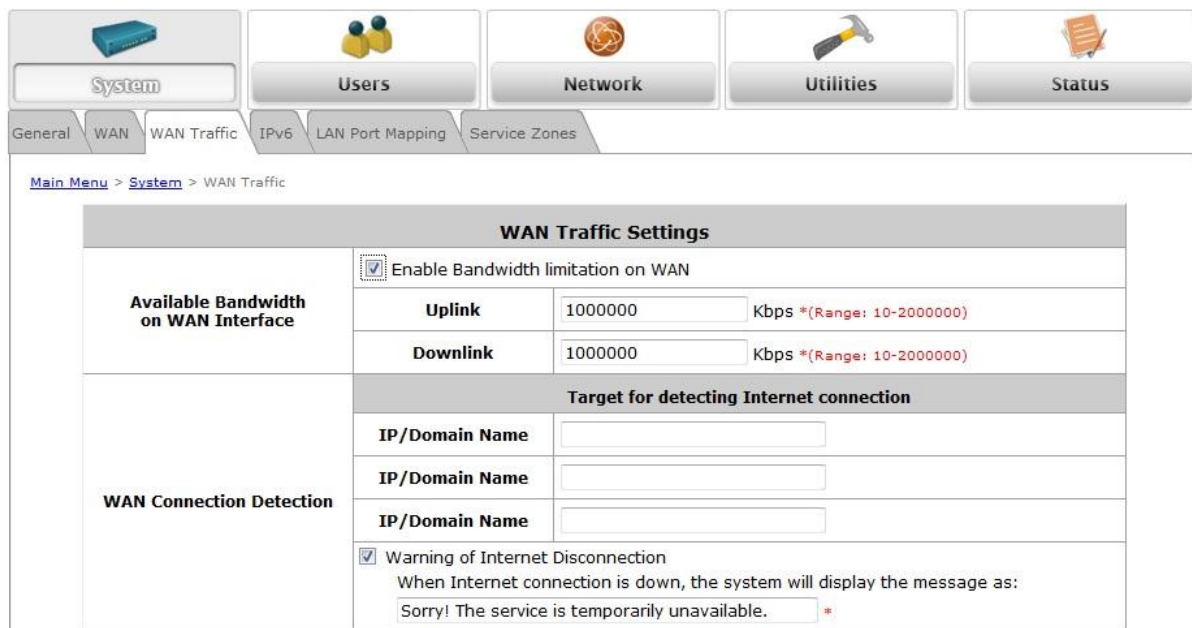
To limit the WAN bandwidth and enable WAN connection detection, click the **Main Menu** button, then **System** and then **WAN Traffic**.

Limiting WAN bandwidth

This feature gives administrators control over the entire system's traffic on the WAN interface. These parameters set here should not exceed the real bandwidth provided by your ISP. For example, if your xDSL is 8Mbps/640kbps, you may input values equal to or less than the speed here.

Available Bandwidth on WAN Interface:

-  **Uplink:** Specifies the maximum uplink bandwidth that can be shared by clients of the system.
-  **Downlink:** Specifies the maximum downlink bandwidth that can be shared by clients of the system.



The screenshot shows the NetComm Wireless web interface. At the top, there are five main menu buttons: System, Users, Network, Utilities, and Status. Below these, there are sub-menu buttons: General, WAN, WAN Traffic, IPv6, LAN Port Mapping, and Service Zones. The 'WAN Traffic' sub-menu is selected, and the breadcrumb trail shows 'Main Menu > System > WAN Traffic'.

The 'WAN Traffic Settings' section is displayed. It includes a checkbox for 'Enable Bandwidth limitation on WAN' which is checked. Below this, there are two rows for bandwidth settings:

Available Bandwidth on WAN Interface	Uplink	Downlink
	1000000 Kbps *(Range: 10-2000000)	1000000 Kbps *(Range: 10-2000000)

Below the bandwidth settings, there is a section for 'WAN Connection Detection' with a sub-header 'Target for detecting Internet connection'. It contains three input fields for 'IP/Domain Name' and a checkbox for 'Warning of Internet Disconnection' which is checked. Below the checkbox, there is a text field for the warning message: 'Sorry! The service is temporarily unavailable.' with a red asterisk indicating a required field.

Enabling WAN connection detection

When this function is enabled, the gateway will try to access these IP/Domain addresses. If the gateway can reach these IP/Domain addresses, the Internet connection is deemed to be functioning normally.

WAN Connection Detection:

-  **IP/Domain Name:** Enter the IP address or domain name that the gateway will use to verify the internet connection status.

The **Warning of Internet Disconnection** option allows you to specify a message that is displayed on a user's screen when they access a web page and the internet connection is down.

Configuring Zones

To configure a Zone, go to: **System >> Service Zones**.

A Zone is a logical network area that covers wired or wireless networks, or both of them. The zones effectively separate the gateway into two distinct networks which are controlled through the use of authentication, security features, wireless encryption methods and traffic control.

The two zones on the gateway are Private Zone and Public Zone, as shown in the table below. Private Zone means clients are not required to be authenticated before using the network service while clients in Public Zone are required to obtain authentication before using the service.



System



Users



Network



Utilities



Status

General

WAN

WAN Traffic

IPv6

LAN Port Mapping

Service Zones

[Main Menu](#) > [System](#) > Service Zone

Service Zone Settings

Service Zone Name	Applied Policy	IP Address	Network Alias	DHCP Pool	LAN Port Mapping	Details
	Default Authen Option	IPv6 Address			Status	
Private	Policy 1	192.168.1.254	N/A	192.168.1.1 ~ 192.168.1.100		Configure
	Disabled	N/A			Enabled	
Public	Policy 1	172.21.0.254	N/A	172.21.0.1 ~ 172.21.0.100		Configure
	Server 1	N/A			Enabled	

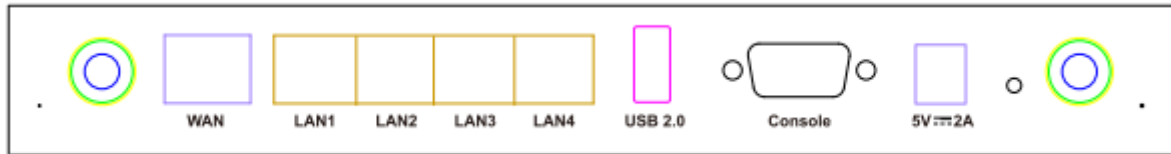
-  **Service Zone Name:** Name of the Zone.
-  **Applied Policy:** Current policy that is applied to the Zone.
-  **Default Authen Option:** Default authentication method/server that is used within the Zone.
-  **IP/IPv6 address:** Shows the LAN IP address. IPv6 is support and can be configured from the IPv6 tab.
-  **Network Alias:** Shows the IP address that bridges to different subnets configured in the Network Alias List.
-  **DHCP Pool:** Shows the range of LAN IP address which clients are assigned to get from DHCP.
-  **LAN Port Mapping:** Each physical LAN port can be set individually to map to a specific zone, and can be configured from the LAN Port Mapping tab (refer to 3.5.1).
-  **Status:** Shows the Private/Public Zone mappings to the physical LAN ports.
-  **Details:** Configurable, detailed settings for each Zone.

Click the **Configure** button to configure each Zone: Basic Settings, Authentication Settings, Wireless Settings, and WDS Settings (Public Zone only).

Port Role Assignment

The gateway supports two zones, Private and Public. In the Private Zone, authentication is not required to access the network, whether it is via wired and wireless connection. In the Public Zone, the **"Authentication Required for Zone"** option is enabled by default, so clients have to be authenticated successfully before surfing the Internet.

The Zone and Port mappings are shown below, LAN1, LAN2 maps to Private Zone and LAN3, LAN4 to Public Zone respectively.



Note: The gateway's web-based user interface can also be accessed via WAN port as long as the administrator uses an IP address listed on the Management IP Address List (Go to **System >> General >> Management IP Address List**). If both WAN and LAN ports are unable to reach the user interface, please use console interface to resolve this issue.

Configure Zone Network

To configure a Zone network, go to: **System >> Service Zones**.

General	WAN	WAN Traffic	IPv6	LAN Port Mapping	Service Zones	Layer 2 Firewall
Main Menu > System > Service Zone						
Service Zone Settings						
Service Zone Name	Applied Policy	IP Address	Network Alias	DHCP Pool	LAN Port Mapping	Details
	Default Authen Option	IPv6 Address			Status	
Private	Policy 1	192.168.110.1	N/A	192.168.110.2 ~ 192.168.110.100		Configure
	Disabled	N/A			Enabled	
Public	Policy 1	192.168.120.1	N/A	192.168.120.2 ~ 192.168.120.100		Configure
	Server 1	N/A			Enabled	

General

WAN

WAN Traffic

IPv6

LAN Port Mapping

Service Zones

Layer 2 Firewall

[Main Menu](#) > [System](#) > [Service Zone](#) > [Service Zone Configuration](#) > DHCP Configuration

DHCP Server Configuration for Service Zone Private

DHCP Pool 1	Start IP Address	192.168.110.2	*
	End IP Address	192.168.110.100	*
	Preferred DNS Server	192.168.110.1	*
	Alternate DNS Server		
	Domain Name	domain.com	
	WINS Server		
	Lease Time	1440	* 2 minutes ~ 10080 minutes (7 days)
	Ignore Client Name	☐ Enable ☒ Disable	
DHCP Pool 2	☐ Enable ☒ Disable		

Network Interface:

-  **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, service zone runs in NAT mode. When Router mode is chosen, this zone runs in Router mode.
-  **IP Address:** The IP Address of this zone.
-  **Subnet Mask:** The subnet Mask of this zone.

DHCP Server: Related information needed for setting up the DHCP Server is listed here. To further configure the DHCP Server, click the button **Configure**. Please note that when “*Enable DHCP Relay*” is enabled, the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this zone.

-  **Start IP Address / End IP Address:** A range of IP addresses that the built-in DHCP server will assign to clients.

Note: please change the Management IP Address List accordingly (at *System >> General >> Management IP Address List*) to permit the administrator to access the gateway admin page after the default IP address of the network interface is changed.

-  **Preferred DNS Server:** The primary DNS server that is used by this Zone.
-  **Alternate DNS Server:** The substitute DNS server that is used by this Zone.
-  **Domain Name:** Enter the domain name for this zone.
-  **WINS Server:** The IP address of the WINS (Windows Internet Naming Service) server if WINS server is applicable to this zone.
-  **Lease Time:** This is the time period when the IP addresses issued from the DHCP server will be valid and available.
-  **Reserved IP Address List:** Each zone can reserve up to 40 IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with a certain MAC address.

Configuring the Wireless Network

Wireless General Settings

To configure Wireless General Settings, go to: **System >> Service Zones**. Click the button **Configure** for **Private zone** for further configuration.

Wireless General Settings	
Band	802.11g+802.11n ☐ Pure 11n
Short Preamble	☒ Enable ☐ Disable
Short Guard Interval	☒ Enable ☐ Disable
Channel Width	20 MHz
Channel	1
Max Transmit Rate	Auto
Transmit Power	Highest
DTIM Period	1 (1-255ms)
ACK Timeout	100 (0-255ms)

Wireless General Settings:

- Band:** There are 4 modes from which you may select, **802.11b** (2.4G, 1~11Mbps), **802.11g** (2.4G, 54Mbps), **802.11b+g**, and **802.11g+n**. Select the **Pure 11n** option to configure the gateway to use only the 11n band.
- Short Preamble:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select **Enable** for **Short Preamble** or **Disable** for **Long Preamble**.
- Short Guard Interval (802.11g+n only):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. With 802.11n, short guard interval is half of what it is used to be to increase throughput. Select **Enable** to use Short Guard Interval or **Disable** to use normal Guard Interval.
- Channel Width (802.11g+n only):** For 802.11n, doubling channel bandwidth to 40 MHz is supported to enhance throughput.
- Channel:** Select the appropriate channel from the drop-down menu to correspond with your network settings, for example, Channel 1-11 is available in North American and Channel 1-13 in Europe, or choose the default **Auto**.
- Max Transmit Rate:** The available range is from 1 to 300Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speeds or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- Transmit Power:** Keep the default setting, or select from range to make the Access Point use different transmit power as you wish.
- DTIM Period:** The DTIM Interval specifies the interval at which the delivery traffic indication message is sent out to synchronise the network. A higher DTIM allows the wireless client to save energy, but throughput is decreased.
- ACK Timeout:** The time interval for waiting for the "acknowledgement (ACK) frame". If the ACK is not received within the interval then the packet will be re-transmitted. A higher ACK Timeout interval will decrease the packet lost, but the throughput will be decreased.

Zone Wireless Settings

Each zone has its own VAP (Virtual Access Point) and corresponds to one SSID. In the Private zone, it's VAP1 and the SSID is hidden, so public users will not see this SSID during a scan of available networks. Privileged users may manually add this network by entering the SSID. The SSID of VAP2 under the Public zone is enabled by default with the SSID Broadcast feature, allowing public users to scan for this network.

After you have completed the wireless general settings, configure the specific settings of each zone.

To configure Zone Wireless Security, go to: **System >> Service Zones**, click **Configure** for Private zone or click **Configure** for Public zone.

Wireless Settings :RF1 VAP 1	
Basic	VAP Status : ☒ Enable ☐ Disable ESSID : NetComm_HS1200N_2 *
Security	Security Type : WPA-PSK Cipher Suite : AES (WPA2) Pre-shared Key / Pass-phrase : a1b2c3d4e5 Group Key Update Period : 600 second(s)
Advanced	Beacon Interval : 100 (25-500ms) RTS Threshold : 2346 (1-2346) Fragment Threshold : 2346 (256-2346) Broadcast SSID : ☐ Enable ☒ Disable Station Isolation : ☐ Enable ☒ Disable WMM : ☒ Enable ☐ Disable IGMP Snooping : ☐ Enable ☒ Disable

Wireless Settings: VAP1 (Wireless Settings Private Zone)

-  **Basic:** Enable the VAP Status if you wish to provide a wireless service under this zone. Assign an ESSID to VAP1 under Private Zone or use the default. The ESSID of the Private Zone will not be broadcast and internal staff will need to associate to Private Zone's VAP1 manually.
-  **Security:** Configure the wireless network under Private Zone with security encryption to prevent unauthorised wireless association if necessary. The supported encryption standards are WEP and WPA-PSK.
 -  **WEP:**
 - 802.11 Authentication: Select from Open System or Shared Key.
 - WEP Key Length: Select from 64-bit, 128-bit, 152-bit key length.
 - WEP Key Format: Select from ASCII or Hex format for the WEP key.
 - WEP Key Index: Select a key index from 1~4. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
 - WEP Keys: Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.
 -  **WPA-PSK:**
 - Cipher Suite: Select an encryption method from TKIP (WPA), AES (WAP2), or Mixed.
 - Pre-shared Key / Pass-phrase: Enter the key value for the pre-shared key or pass-phrase.
 - Group Key Update Period: The time interval for the Group Key to be renewed; the time unit is in seconds.
-  **Advanced:** The parameters in Advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.
-  **Beacon Interval:** Enter the number of interval that the beacon signal will be sent from the VAP. The default value is set at 100ms.
-  **RTS Threshold:** Enter a value between 1 and 2346. The RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent hidden node problems. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be

useful in areas where many client devices are associating with the gateway or in areas where the clients are far apart and can detect only the gateway but not each other. The default value is set at 2346.

-  **Fragment Threshold:** Enter a value between 256 and 2346. The default value is 2346. A packet size larger than this threshold, will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.
-  **Broadcast SSID:** The administrator has the option of enabling or disabling the SSID for VAP1 which is the Private Zone. The default value is set to **Disable** where users will not be able to scan for the SSID.
-  **Station Isolation:** By enabling this function, all stations wirelessly associated to this zone are isolated from one another and can only communicate with the gateway.
-  **WMM:** Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.
-  **IGMP Snooping:** IGMP is a multicast constraining mechanism which may flood the broadcast domain. This is effective for dense internet usage such as conventions or campuses.

VAP2 is configured under the Public Zone to provide wireless service to public clients in a hotspot environment. To configure Public Zone's Wireless Settings, click on **Main Menu** then **System** and then **Service Zones**. Click **Configure** for the Public zone.

Wireless Settings :RF1 VAP 2	
Basic	VAP Status : ☒ Enable ☐ Disable ESSID : HS1200N Demo *
Security	Security Type : None
Advanced	Beacon Interval : 100 (25-500ms) RTS Threshold : 2346 (1-2346) Fragment Threshold : 2346 (256-2346) Broadcast SSID : ☒ Enable ☐ Disable Station Isolation : ☐ Enable ☒ Disable WMM : ☒ Enable ☐ Disable IGMP Snooping : ☐ Enable ☒ Disable

Wireless Settings: VAP2 (Wireless Settings for Public Zone)

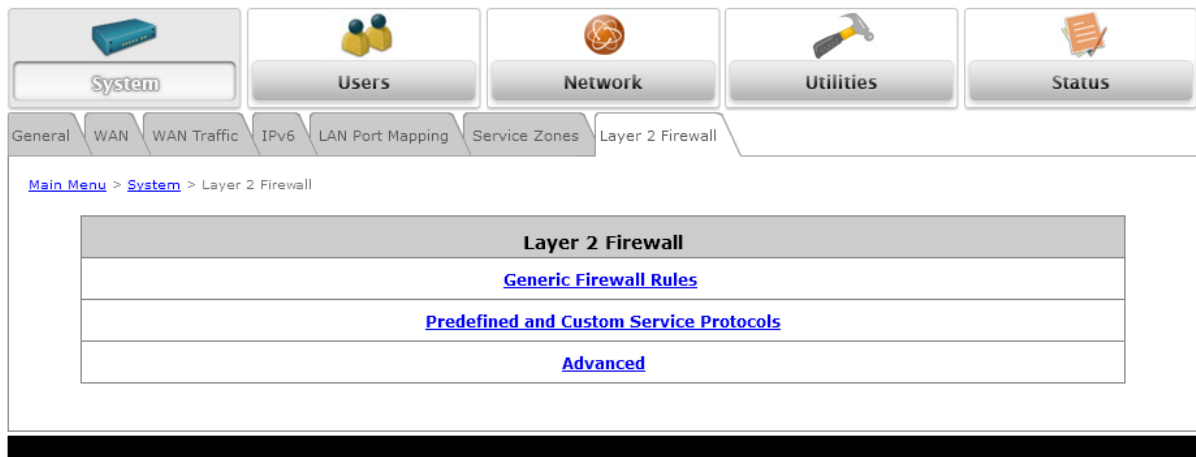
-  **Basic:** Enable the VAP Status if you wish to provide a wireless service under this zone. Assign an ESSID to VAP2 under Public Zone or use the default. The ESSID of the Public Zone is broadcasted so that public users can perform a scan for this network.
-  **Security:** Configure the wireless network under Public Zone with security encryption to prevent unauthorised wireless association if necessary. The supported encryption standards are WEP and WPA-PSK.
 -  **WEP:**
 - 802.11 Authentication: Select from Open System or Shared Key.
 - WEP Key Length: Select from 64-bit, 128-bit, 152-bit key length.
 - WEP Key Format: Select from ASCII or Hex format for the WEP key.
 - WEP Key Index: Select a key index from 1~4. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
 - WEP Keys: Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.
 -  **WPA-PSK:**
 - Cipher Suite: Select an encryption method from TKIP (WPA), AES (WAP2), or Mixed.
 - Pre-shared Key / Pass-phrase: Enter the key value for the pre-shared key or pass-phrase.
 - Group Key Update Period: The time interval for the Group Key to be renewed; the time unit is in seconds.
-  **Advanced:** The parameters in Advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.

- 📶 **Beacon Interval:** Enter the number of intervals that the beacon signal will be sent from the VAP. The default value is set at 100ms.
- 📶 **RTS Threshold:** Enter a value between 1 and 2346. The RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent hidden node problems. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the gateway or in areas where the clients are far apart and can detect only the gateway but not each other. The default value is set at 2346.
- 📶 **Fragment Threshold:** Enter a value between 256 and 2346. The default value is 2346. A packet size larger than this threshold, will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.
- 📶 **Broadcast SSID:** The administrator has the option of enabling or disabling the SSID for VAP2 which is the Public Zone. The default value is set to **Enable** where users will be able to scan for the SSID.
- 📶 **Station Isolation:** By enabling this function, all stations wirelessly associated to this zone are isolated from one another and can only communicate with the gateway.
- 📶 **WMM:** Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.
- 📶 **IGMP Snooping:** IGMP is a multicast constraining mechanism which may flood the broadcast domain. This is effective for dense internet usage such as conventions or campuses.

Wireless Layer 2 firewall

The gateway has a Layer2 Firewall in addition to the standard wireless security. The Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffic, providing another line of defence against possible security threats on the wireless network.

To access the Layer 2 firewall settings, go to **Network >> Layer 2 Firewall**.



Generic Firewall Rules

You can choose to enable or disable the wireless Generic Firewall. This section provides an overview of firewall rules for the system's wireless interface; 6 default rules with up to a total 20 firewall rules are available for configuration.

Firewall Rules						
No.	Active	Action	Rule Name	Ether Type	Remark	Operation
1	☒	Block	CDP	IEEE 802.3		Edit Move to Insert Before Delete
2	☒	Block	STP	IEEE 802.3		Edit Move to Insert Before Delete
3	☒	Block	GARP	IEEE 802.3		Edit Move to Insert Before Delete
4	☒	Block	RIP	IPv4		Edit Move to Insert Before Delete
5	☒	Block	HSRP	IPv4		Edit Move to Insert Before Delete
6	☒	Block	OSPF	IPv4		Edit Move to Insert Before Delete
7	☐	Block	rule 7	ANY		Edit Move to Insert Before Delete
8	☐	Block	rule 8	ANY		Edit Move to Insert Before Delete
9	☐	Block	rule 9	ANY		Edit Move to Insert Before Delete
10	☐	Block	rule 10	ANY		Edit Move to Insert Before Delete

(Total:10) [First](#) [Prev](#) [Next](#) [Last](#)

From the overview table, each rule is designated with the following field;

-  **No.:** The numbering will decide the priority of which the system will carry out the available firewall rules in the tables.
-  **Active:** Checking this field will mark the rule as active which means this rule will be enforced.
-  **Action:** **Block** denotes a block rule; **PASS** denotes a pass rule.
-  **Rule Name:** This is the denominated name of the rule.
-  **EtherType:** It denotes the type of traffic subjected to this rule.
-  **Remark:** It shows the additional reference information of this rule.
-  **Operation:** 4 actions are available; **Edit** denotes to edit the rule details, **Move to** denotes to move the rule to a specified rule number, **Insert Before** denotes to insert a rule before the current rule, and **Delete** denotes to delete the rule.

To edit a specific rule:

Click **Edit** in the **Operation** column of the firewall rules table. On this page, existing rules may be edited.

General
WAN
WAN Traffic
IPv6
LAN Port Mapping
Service Zones
Layer 2 Firewall

[Main Menu](#) > [System](#) > Layer 2 Firewall

Edit Filter Rule	
Rule Number	1
Rule Name	CDP
Action for Matched Packets	☐ Pass ☒ Block
Rule Remark	

Link Layer Configuration	
Ether Type	IEEE 802.3
Interface	☒ From ☐ To VAP2
Source	Destination
MAC Address	01:00:0C:CC:CC:CC
MAC Mask	

IEEE 802.3 Configuration	
DSAP / SSAP	aa
SNAP Type	2000 For example IP: 0800

Apply
Cancel

- Rule Number:** The numbering of this specific rule will decide its priority among available firewall rules on the list.
- Rule name:** Enter the rule name.
- Action for Matched Packets:** The rule can be chosen to **Block** or **Pass** packets that match the rule criteria.
- Rule Remark:** Enter any comments regarding the rule that help to identify it.
- Ether Type:** Select from the drop down list which types of traffics are subject to this rule.
- Interface:** For specifying the traffic direction (To or From VAP2) subjected to this rule.
- IPv4 Service** (when EtherType is **IPv4**): Select the available upper layer protocols/services from the drop down list.
- DSAP/SSAP** (when EtherType is **IEEE 802.3**): The value can be further specified for the fields in 802.2 LLC frame header.
- SNAP Type** (when EtherType is **IEEE802.3**): The field can be used to indicate the type of encapsulated traffic.
- Opcode** (when EtherType is **ARP**): This list can be used to specify the ARP Opcode in ARP header.
- Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).
- Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).

When you have finished making changes, click the **Apply** button so that the changes can take effect.

To add a new rule,

Select the **Insert Before** link in the **Operation** column of the firewall list.

General
WAN
WAN Traffic
IPv6
LAN Port Mapping
Service Zones
Layer 2 Firewall

[Main Menu](#) > [System](#) > Layer 2 Firewall

Edit Filter Rule

Rule Number	1
Rule Name	default rule
Action for Matched Packets	☐ Pass ☒ Block
Rule Remark	

Link Layer Configuration

Ether Type	All
Interface	☒ From ☐ To VAP2

Source	Destination
MAC Address	MAC Address
MAC Mask	MAC Mask

To move a specific rule,

Select the **Move to** option in the **Operation** column of the firewall rule then select the number that you would like to move it to. Click **OK** to save the changes made.

Move to No. 5

Please make sure all the desired rules are checked as Active and click the **Apply** button below on the overview page.

General
WAN
WAN Traffic
IPv6
LAN Port Mapping
Service Zones
Layer 2 Firewall

[Main Menu](#) > [System](#) > Layer 2 Firewall

Generic Firewall

☒ Enable
☐ Disable

Firewall Rules

No.	Active	Action	Rule Name	Ether Type	Remark	Operation
1	☒	Block	CDP	IEEE 802.3		Edit Move to Insert Before Delete
2	☒	Block	STP	IEEE 802.3		Edit Move to Insert Before Delete
3	☒	Block	GARP	IEEE 802.3		Edit Move to Insert Before Delete

Predefined and Custom Service Protocols

The administrator can add or delete firewall service protocols here; the services on this list will become available drop down options to choose from in the firewall rules (when EtherType is IPv4).

The first 27 entries are default services and the administrator can add any extra desired services. These 27 default firewall services cannot be deleted but can be disabled.

General
WAN
WAN Traffic
IPv6
LAN Port Mapping
Service Zones
Layer 2 Firewall

[Main Menu](#) > [System](#) > Layer 2 Firewall

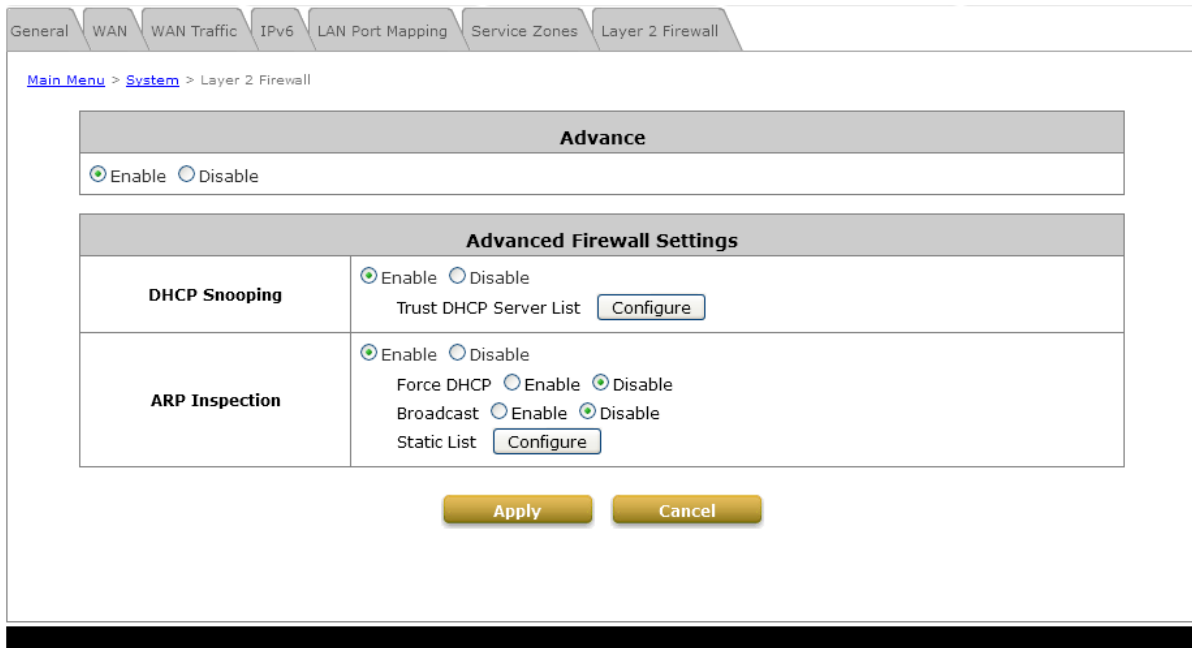
Service Protocols			
No.	Name	Description	Select All
1	ALL	ALL	☐
2	ALL TCP	TCP, Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL ICMP	ALL ICMP	☐
4	FTP	TCP/UDP, Destination Port: 20~21	☐
5	HTTP	TCP/UDP, Destination Port: 80	☐
6	HTTPS	TCP/UDP, Destination Port: 443	☐
7	POP3	TCP, Destination Port: 110	☐
8	SMTP	TCP, Destination Port: 25	☐
9	DHCP	UDP, Destination Port: 67~68	☐
10	DNS	TCP/UDP, Destination Port: 53	☐

Add
Delete

(Total: 27) [First](#) [Prev](#) [Next](#) [Last](#)

Advanced

Advanced Firewall Settings can be enabled to supplement the firewall rules, providing extra security enhancement against DHCP and ARP traffic traversing the available interfaces of the system.



General WAN WAN Traffic IPv6 LAN Port Mapping Service Zones **Layer 2 Firewall**

Main Menu > System > Layer 2 Firewall

Advance

☒ Enable ☐ Disable

Advanced Firewall Settings

DHCP Snooping	☒ Enable ☐ Disable Trust DHCP Server List Configure
ARP Inspection	☒ Enable ☐ Disable Force DHCP ☐ Enable ☒ Disable Broadcast ☐ Enable ☒ Disable Static List Configure

[Apply](#) [Cancel](#)

-  **DHCP Snooping:** When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack. In addition, the **Trusted DHCP List** (IP/MAC) can be used to specify legitimate DHCP servers to prevent rogue DHCP servers.
-  **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing.
 -  **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any client with a static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static List**.
 -  **Broadcast** can be enabled to let other access points (with an L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests.
 -  **Static List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests; however, if their IP appears on the static list (with a different MAC), their ARP requests will be dropped to prevent eavesdropping.

If any settings are changed, please click **Apply** to save the configuration before leaving this page.

Configuring network access

Type of Users

To configure Users, go to **Users >> Authentication**.

This section is for administrators to pre-configure authentication servers for the entire system. Concurrently up to three servers can be selected and pre-configured for static user authentication. One server uses built-in LOCAL database while the other two servers use external RADIUS database. In addition, 'ONDEMAND' server can be configured for temporary user authentication.

Authentication Settings		
Auth Option	Auth Database	Postfix
Server 1	LOCAL	local
Server 2	RADIUS	radius1
Server 3	RADIUS	radius2
On-demand User	ONDEMAND	ondemand
FREE	FREE	N/A

- Authentication Settings:** There are four different authentication options on the gateway that use databases: **LOCAL**, **RADIUS1**, **RADIUS2**, **ONDEMAND** and **FREE**. **Local** and **On-demand** are built in databases with user credentials stored locally, and **RADIUS** is one of the most common external authentication databases. **FREE** is an access option that allows users to access networks with any specified identity token on the login page. Click on the Authentication Options to configure.
- Auth Option:** Set a name for the authentication databases by using numbers (0~9), alphabet (a~z or A ~Z), dash (-), underscore (_), space and dot (.) only. This name is used for the administrator to easily identify the authentication options such as HQ-RADIUS.
- Postfix:** A postfix represents the authentication server in a complete username. For example, **user1@local** means that this user (user1) will be authenticated by the LOCAL authentication database.
- Black List:** There are 5 sets of black lists provided by the system. A user account listed on the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one (or None) black list from the drop down menu and it will be applied to this specific authentication option.
- Configure:** Click the **Configure** button to edit a specific authentication database for the server. For example, if you want to edit the *Local* authentication database, please click the **Configure** button for **Local**.

Local

Click the **Configure** button for **Local** for further configuration.

Local User Database Settings	
Local User List	
Account Roaming Out	☐ Enable ☒ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	☐ Enable ☒ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

Local User List: Allows the administrator to view, add or delete local user accounts. The **Upload User** button is for importing a list of user accounts from a text file. The **Download User** button is for exporting all local user accounts into a text file. Clicking the hyperlink of a user account leads to a page for configuration.

Local User List					
Username	Password	Applied Group	MAC Address		Del All
		Account Status	Begin Date	End Date	
		Remark			
user1	user1	Group 1			Delete
		Valid			

(Total:1/500) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

Add User: Click this button to enter the **Adding User(s) to the List** interface. Fill in the necessary information such as **“Username”**, **“Password”**, **“MAC Address”**, **“Remark”** and login **“Schedule”**. Select a desired **Group** to classify local users. Click **Apply** to complete adding the user(s). MAC address of a networking device can be bound with a local user as well. It means this user must log in to the system with a networking device (namely PC) that has the corresponding MAC address. That is, this user can not log in with other networking devices. An expiration time can be enabled for the user.

Adding User(s) to the List								
No.	Username*	Password*	MAC Address (XX:XX:XX:XX:XX:XX)	Group	Remark	Begin Date	End Date	Enable Expire Time
1				Group 1 ▾		Select	Select	☐
2				Group 1 ▾		Select	Select	☐
3				Group 1 ▾		Select	Select	☐
4				Group 1 ▾		Select	Select	☐
5				Group 1 ▾		Select	Select	☐
6				Group 1 ▾		Select	Select	☐
7				Group 1 ▾		Select	Select	☐
8				Group 1 ▾		Select	Select	☐

Search: Enter a keyword of a username or remark to be searched in the text file and click this button to perform the search. All usernames matching the keyword will be listed.

Local User List					
Username	Password	Applied Group	MAC Address		Del All Delete
		Account Status	Begin Date	End Date	
		Remark			
user1	user1	Group 1			
		Valid			

(Total:1/500) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

Del All: Click this button to delete all the users at once or click **Delete** (hyperlinked) to delete a specific user individually.

Edit User: Click the desired user account on the **Local User List** to enter the **User Profile** Interface for that particular user, and then modify or add information such as Username, Password, MAC Address (optional), Applied Group (optional) and Remark (optional). An expiration time can be enabled and the Begin/End Date can be selected. Click **Apply** to complete the modification.

Authentication		Black List	Group	Policy	Schedule	Firewall	QoS	Specific Route	Privilege	Additional Control	Operator
Main Menu > Users > Authentication > Option > Local > Local User List > Editing User											
Editing Existing User Data											
Username	user01 *										
Password	123 *										
MAC Address											
Applied Group	Group 1 ▼										
Remark											
Enable Expire Time	☐										
Begin Date	Select Date										
End Date	Select Date										

RADIUS

There are two RADIUS authentication databases for configuration. Click **Configure** for any one of **RADIUS** servers for further configuration. The RADIUS server sets the external authentication for user accounts. Enter the information concerning the primary server and/or the secondary server (the secondary server is not mandatory). The fields with red asterisks are mandatory fields. These settings will become effective immediately after clicking **Apply**.

External RADIUS Server Related Settings		
802.1X Authentication	☐ Enable ☒ Disable	
Username Format	☒ Leave Unmodified ☐ Complete (e.g. user1@postfix) ☐ Only ID (e.g. user1)	
NAS Identifier		
NAS Port Type	19 *(Default 19, Range: 0~35)	
Accounting Delay Time	0 *(Default: 0)	
Service Type	1 *(Default: 1, Range: 1~11)	
Class-Group Mapping	Configure	
DM & CoA Settings	Configure	
Acct Interim for users' IP changed	☐ Enable ☒ Disable (Acct Interim is sent when users' IP are changed if Enable)	
Failover between RADIUS Servers	☐ Enable ☒ Disable	
Attributes Priority	Follow Server's Setting v	
	Standard RADIUS Attributes	
	Session Timeout	240 Minutes *(Range: 5-1440 mins)
	Idle Timeout	10 Minutes *(Range: 1-120 mins)
	Acct Interim Interval	15 Minutes *(Range: 1~120 mins, 0 is disable)
	WISPr Vendor Specific Attributes	
	Redirection URL	
	Billing Class Of Service	
	Session Terminate on Billing Time	☐ Enable ☒ Disable
	Session Terminate Time	Never
Retransmission Settings	Bandwidth Setting	Group 1
	Number of Retries	3 *(Default: 3)
	Timeout	6 *(Default: 6)
Primary RADIUS Server		
Authentication Server	*(Domain Name/IP Address)	
Authentication Port	*(Default: 1812)	
Authentication Secret Key	*	
Authentication Protocol	CHAP v	
Accounting Service	☒ Enable ☐ Disable	
Accounting Server	*(Domain Name/IP Address)	
Accounting Port	*(Default: 1813)	
Accounting Secret Key	*	
Secondary RADIUS Server		
Authentication Server	(Domain Name/IP Address)	
Authentication Port		
Authentication Secret Key		
Authentication Protocol	CHAP v	
Accounting Service	☒ Enable ☐ Disable	
Accounting Server	(Domain Name/IP Address)	
Accounting Port		
Accounting Secret Key		

External RADIUS Related Settings

-  **802.1X Authentication:** Enable /Disable 802.1X authentication for users authenticated through this Server.
-  **Username Format:** Select the format of the user login information required to be sent to the external RADIUS Server. You may choose to send the username in **Complete** (userID + Postfix), **Only ID** or **Leave Unmodified**. Please note that if the Leave Unmodified option is selected, the system will send the input as is.
-  **NAS Identifier:** This attribute is the string identifying the NAS originating the access request. System will send this value to the external RADIUS server, if the external RADIUS server needs this.
-  **NAS Port Type:** Indicates the type of physical port the network access server is using to authenticate the user. System will send this value to the external RADIUS server, if the external RADIUS server needs this.
-  **Account Delay Time:** This attribute adds flexibility for the gateway to process accounting requests in the time specified. Default is set at 0.
-  **Service Type:** This attribute indicates the type of service the user has requested or the type of service to be provided, required for some RADIUS servers that only accepts specified service types.
-  **Class-Group Mapping:** This function is to impose a Group on a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to an assigned Group.

RADIUS Group Mapping - Server 2				
☐ Enable ☒ Disable				
No.	Class Attribute Value	Group	Remark	
1		Group 1 ▼		
2		Group 1 ▼		
3		Group 1 ▼		
4		Group 1 ▼		
5		Group 1 ▼		

-  **DM & CoA Settings:** This function allows administrator to assign users to receive Disconnect Messages / Change of Authorization from the server and sessions can be terminated instantly. Click **Configure** to enter the IP addresses of the users.
-  **Attributes Priority:** This section shows the Standard RADIUS attributes which include Session Timeout, Idle Timeout and Acct Interim Interval; and WISPr Vendor Specific Attributes. These attributes are predetermined, and if needed, choose Overwrite Server's Setting to make changes.

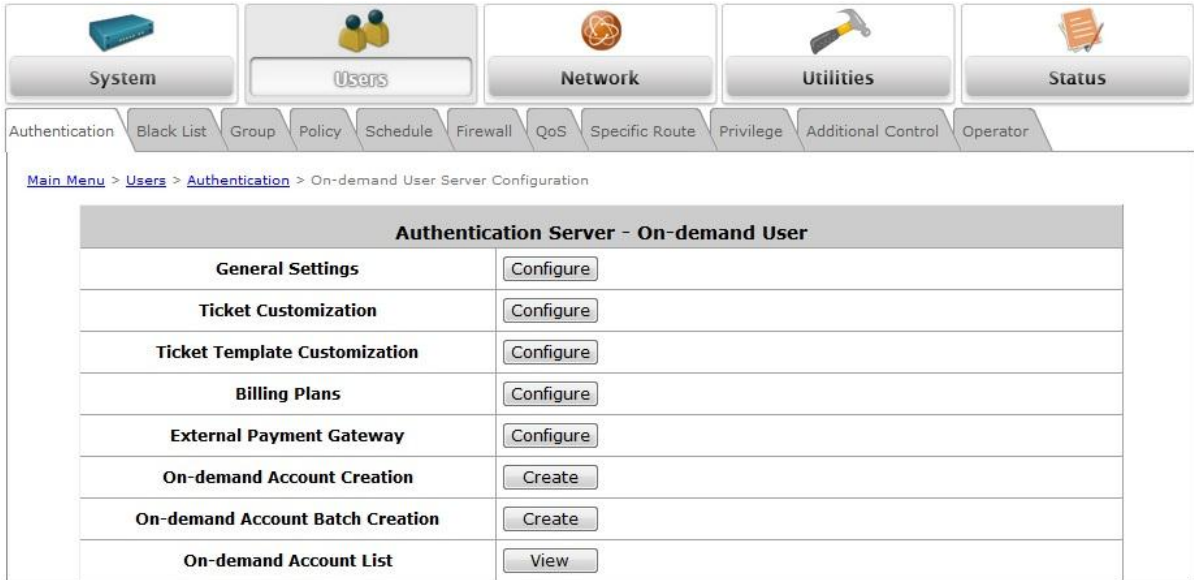
Primary / Secondary RADIUS Server

-  **Authentication Server:** Enter the domain name or IP address of your RADIUS Server.
-  **Authentication Port:** Enter the Port number used for authentication.
-  **Accounting Port:** Enter the Port number used for accounting.
-  **Authentication Secret Key:** Secret Key used for authentication.
-  **Accounting Service:** Enable / Disable RADIUS accounting.
-  **Accounting Server:** Enter the domain name or IP of your accounting server
-  **Authentication Protocol:** Select Challenge-Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
-  **Accounting Secret Key:** The key between the RADIUS server and the gateway to test the authenticity of the link.

On-Demand User

On-demand User Server Configuration:

The administrator can configure this authentication method to create on-demand user accounts. This function is designed for hotspot owners to provide temporary users with free or paid wireless Internet access in the hotspot environment. Major functions include accounts creation, users monitoring list, billing plan and external payment gateway support.



Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Ticket Template Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account Batch Creation	Create
On-demand Account List	View

General Settings

This is the common setting for the On-demand User authentication option.



General Settings	
Postfix	ondemand
Remaining Volume Sync Interval	☒ 10min(s) ☐ 15min(s) ☐ 20min(s)
Terminal Server	Configure
Expired Account Keep Days	15 *(1~30 days)
Out of Quota Account Keep Days	15 *(1~30 days)
Account Roaming Out	☐ Enable ☒ Disable (On-demand user database will be used as authentication database for roaming out users.)

Postfix: The string of characters needed to be entered with the username during login.

Remaining Volume Sync Interval: Select a desired interval for on-demand user quota update. The quota information, i.e. remaining time or remaining quota displayed on the on-demand user login success page will be refreshed according to the time interval configured here.

Terminal Server: Terminal Server Configuration is a list of serial-to-Ethernet devices that communicate with the system only; there is no need to go online or go through authentication process. Enter the device IP and the port number into the respective fields.


System


Users


Network


Utilities


Status

Authentication
Black List
Group
Policy
Schedule
Firewall
QoS
Specific Route
Privilege
Additional Control
Operator

[Main Menu](#) > [Users](#) > [Authentication](#) > [On-demand User Server Configuration](#) > [General Settings](#) > Terminal Server Configuration

Terminal Server Configuration					
Status	Item	Server IP	Port	Location	Remark
●	1				
●	2				
●	3				

Account Roaming Out: When Account Roaming Out is enabled, a link will be available to define the client device authorized to roam by entering the IP address, Subnet Mask, and Secret Key.

Ticket Customization

On-demand account ticket can be customized here and previewed on the screen.

Ticket Customization	
Currency	☐ None ☐ \$ USD ☐ £ GBP ☐ € EUR ☒ AUD (Input other desired monetary unit, e.g. AU)
WLAN ESSID	
Wireless Key	
Receipt Header 1	Welcome to NetComm Wireless
Receipt Header 2	
Receipt Header 3	
Receipt Footer 1	Thank you and enjoy your day
Receipt Footer 2	
Receipt Footer 3	
Remark	
Background Image	☒ None ☐ Default Image ☐ Uploaded Image Edit
Number of Tickets	☒ 1 ☐ 2

Currency: Select the desired currency unit for charged internet access.

WLAN ESSID: Enter a name for the ESSID of the Public Zone.

Wireless Key: The wireless key configured in Public Zone Settings will be shown.

Receipt Header(Optional): There are 3 receipt headers supported by the system. The entered content will be printed on the receipt.

Receipt Footer(Optional): There are 3 receipt footers supported by the system. The entered content will be printed on the receipt.

Remark: Enter additional information that will appear at the bottom of the receipt.

Background Image: You can choose to customize the ticket by uploading your own background image for the ticket, or choose none. Click **Edit** to select the image file and then click **Upload**. The background image file size limit is 100 Kbytes. No limit for the dimensions of the image is set, but a 460x480 image is recommended.

Number of Tickets: Enable this function to print duplicate receipts. Another Remark field will appear when the Number of Tickets is set to 2 and the content will appear at the bottom of the duplicate receipt.

Preview: Click **Preview** to show the ticket, including the username and password with the selected background. You can also print the ticket here.

Ticket Template Customization

Administrators can customise contents on the On-demand tickets using this template.

Template Customization

Image

Type

Type I

Restore

(For Usage-Time with expiration time & Volume)

Template

Type I

Font Size
☒ Normal ☐ Tall

Parameters

\$remain

Insert Parameters

(Ticket Serial Number)

SN: \$remain

\$header
\$2header
\$3header

Username : \$username
Password : \$password
Quota : \$usage
Total Price : \$price
External ID : \$extid

ESSID : \$wlan_ess_id
Wireless Key : \$wep_key

Your first time login must be
done before \$expire_time

The account is valid within
\$duration days
after your first login.

Apply

Clear

Billing Plans

Administrators can configure several billing plans. Click the **Edit** button to enter the **Editing Billing Plan** page. Configure billing plans with the desired account type, expiration date, price, etc. and then click **Apply** to save the plan. On the **Billing Plans** screen, select the **Enable** checkbox or click **Select all**, and then click **Apply** to activate the plan(s).

Billing Plans						
Plan	Account Type	Quota	Price	Enable ☐	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	2.99	☒	Group 1	Edit
2	Duration-time	Valid for 4 hour(s) elapsed time	4.99	☒	Group 2	Edit
3	Volume	100 Mbyte(s) of traffic volume quota	1.99	☒	Group 3	Edit
4	Hotel Cut-off-time	Valid until 23:00 the following day	3.99	☒	Group 4	Edit
5	N/A			☐	Group 1	Edit
6	N/A			☐	Group 1	Edit
7	N/A			☐	Group 1	Edit
8	N/A			☐	Group 1	Edit
9	N/A			☐	Group 1	Edit
0	N/A			☐	Group 1	Edit

Plan: The number of the specific plan.

Type: This is the type of plan, based on which it defines how the account can be used including Usage-time, Volume, Hotel Cut-off and Duration-time.

Quota: The limit on how On-demand users are allowed to access the network.

Price: The unit price charged for buying an account from this billing plan.

Enable: Check the checkbox to activate the plan.

Group: Users under this billing plan will be classified under this group. The default value is Group 1.

Function: Click the **Edit** button to add one billing plan. For detailed information regarding on-demand accounts and billing plan configuration, please refer to **Appendix E, On-demand Account types & Billing Plan**.

External Payment Gateway

This section is for merchants to set up an external payment gateway to accept online payments for wireless internet access.

The available payment services are **Authorize.Net**, **PayPal**, **SecurePay**, **WorldPay** or **Disable**. For detailed parameter descriptions please refer to **Appendix F, External Payment Gateways**.

External Payment Gateway				
☐ Authorize.Net	☐ PayPal	☐ SecurePay	☐ WorldPay	☒ Disable

On-demand Account Creation

After at least one billing plan is enabled, the administrator can generate on-demand user accounts here. Click **Create** from the desired plan to create an on-demand account. The username and password of to-be-created on-demand account is configurable. Select **Manual created** in Username/Password Creation and administrator can enter a desired username and password for the on-demand account. In addition, an External ID such as student's school ID can be entered together with account creation.

After the account is created, you can click **Printout** to print a receipt which will contain the on-demand user's information, including the username and password. Click **Send to POS** to print a receipt on the ticket printer.

Note: If no Billing plan is enabled, accounts cannot be created by clicking Create. Please go back to Billing Plans to activate at least one Billing plan by clicking Edit and Apply to activate the plan. The printer used by Print is a pre-configured printer connected to the administrator's computer.

On-demand Account Creation					
Plan	Account Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	<button>Create</button>
2	Usage-time	11 min(s) connection time quota	1	Enabled	<button>Create</button>
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	<button>Create</button>
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	<button>Create</button>
5	N/A	N/A	N/A	Disabled	<button>Create</button>
6	N/A	N/A	N/A	Disabled	<button>Create</button>
7	N/A	N/A	N/A	Disabled	<button>Create</button>
8	N/A	N/A	N/A	Disabled	<button>Create</button>
9	N/A	N/A	N/A	Disabled	<button>Create</button>
0	N/A	N/A	N/A	Disabled	<button>Create</button>

Plan: The number of a specific plan.

Account Type: Show account type of the plan in Usage-time. Duration-time or Hotel Cut-off.

Quota: The total amount of time, interval or traffic volume for On-demand users to access the network. For Time users, it is the total time. For Volume users, it is the total amount of traffic.

Price: For each plan, this is the unit price charged for an account.

Status: Show the status in enabled or disabled.

Function: Press **Create** for the desired plan; and 'Creating an On-demand Account' will appear for creation.

On-demand Account Creation					
Plan	Account Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create

Creating an On-demand Account	
Plan : Account Type	2 : Usage-time
Quota	11 min(s) of connection time quota
Account Creation	System created ▼
Account Activation	First time login must be done within 1 hour(s)
Total Price	1
Unit	1 Units per ticket
Group	Group 1 ▼
Reference	Add a reference related to this account (for example, the customer's name)
External ID	Enter an external ID such as Library ID No.
Please confirm the information and press Create button to create an account.	

On-demand Account Batch Creation

After at least one billing plan is enabled, the administrator can generate multiple on-demand user accounts at once with batch creation. For potential hotspot operators who may wish to pre-generate guest accounts for sale, the On-demand feature has a batch create functionality which allows the administrator or operator access to the On-demand page, to create multiple accounts for an enabled billing plan and send them to the printer for generating physical tickets.

Batch Creating On-demand Account	
Plan : Account Type	1 : Usage-time
Quota	1 hr(s) of connection time quota with expiration
Numbers	1 Number of tickets to batch create
Account Creation	Manual created ▼
Username	Prefix: *(A-z/0-9 and max length is 5) Serial Number: *(1~5 digits and max length is 5) Postfix: *(A-z/0-9 and max length is 5) *(Total length is less than 10)
Password	☒ Randomly ☐ Same as username ☐ Admin Assign
Valid Period	After activation, the account will be expired in 30 day(s)
Total Price (AUD)	5
Unit	1 Number of units per ticket
Group	Group 1 ▼
Please confirm the information and press Create button to create accounts.	

Account Type: Shows the account type of the plan, whether it is **Usage-time**, **Duration-time** or **Hotel Cut-off**.

Quota: The total amount of time, interval or traffic volume for On-demand users to access the network.

Numbers: The desired number of accounts to be created from the plan.

Username/Password Creation: Usernames and passwords can be created randomly by the gateway or self-created by administrator.

Username: To manually create a username, the Prefix and Postfix can be chosen. The serial number increases at single increments when batch accounts are created.

Password: Passwords are customizable and can be created randomly by the gateway or self-created by administrator.

Valid Period: Shows when the account will expire.

Total Price: For each plan, this is the unit price charged for an account.

Unit: Number of units of Quota per ticket

Group: On-demand users can be allocated to a defined User Group when On-demand accounts are created.

The generated accounts may be downloaded for safe keeping, or sent to printer for batch printout.

On-demand Account Creation by Quick Button

The **Quick Button** located on the front panel of gateway is a quick On-demand account generation button. This button is designed to create On-demand accounts without the need to enter WMI. The printer should be directly connected to the console port of gateway.

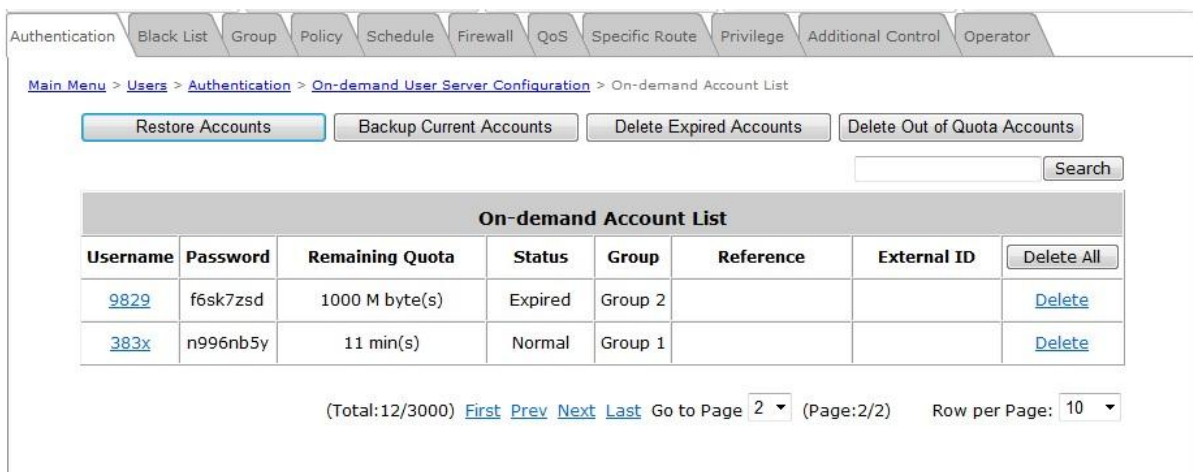
When you have properly connected the printer to the console port, pressing this button will generate an On-demand account using billing plan no.1 and print out the account credentials via the printer.

Please note that the corresponding billing plan no. for this **Quick Print** button is always billing plan 1. Should the network administrator wish to configure different account types for generation, please modify billing plan no.1.

**Only supports normal font for ticket customization.*

On-demand Account List

All created On-demand accounts are listed and related information is also provided.



The screenshot shows the 'On-demand Account List' page. At the top, there are tabs for Authentication, Black List, Group, Policy, Schedule, Firewall, QoS, Specific Route, Privilege, Additional Control, and Operator. Below the tabs is a breadcrumb trail: Main Menu > Users > Authentication > On-demand User Server Configuration > On-demand Account List. There are four buttons: Restore Accounts, Backup Current Accounts, Delete Expired Accounts, and Delete Out of Quota Accounts. A search box with a Search button is also present. The main table is titled 'On-demand Account List' and has columns: Username, Password, Remaining Quota, Status, Group, Reference, External ID, and a Delete All button. The table contains two rows of data. Below the table, there is a summary line: (Total:12/3000) First Prev Next Last Go to Page 2 (Page:2/2) Row per Page: 10.

Username	Password	Remaining Quota	Status	Group	Reference	External ID	Delete All
9829	f6sk7zsd	1000 M byte(s)	Expired	Group 2			Delete
383x	n996nb5y	11 min(s)	Normal	Group 1			Delete

(Total:12/3000) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:2/2) Row per Page:

Search: Enter a keyword of a username, External ID, or reference, to be searched in the text file and click this button to perform the search. All usernames, External ID, or reference, matching the keyword will be listed.

Username: The login name of the account.

Password: The login password of the account.

Remaining Quota: The remaining time or volume, or the cut-off time that the account can continue to use to access the network.

Status: The status of the account.

Normal: the account is not currently in use and has not exceeded the quota limit.

Online: the account is currently in use.

Expired: the account is not valid any more, even if there is remaining quota left.

Out of Quota: the account has exceeded the quota limit.

Redeemed: the account has been applied for account renewal.

External ID: This is an additional information field combined with a unique account, for example the customer's name or social security number etc.

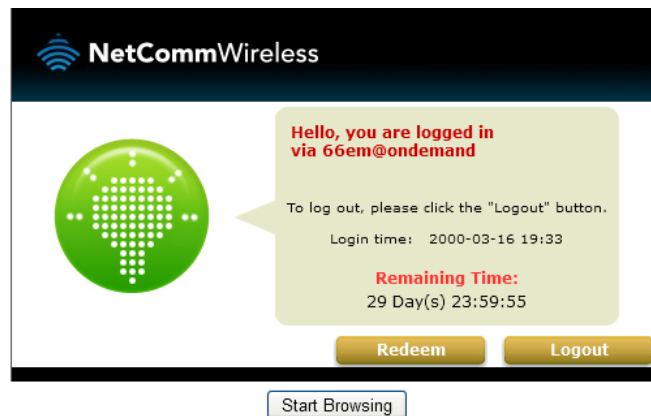
Reference: Any other additional information, for example venue where the account is generated etc.

Delete All: This deletes all user accounts.

Delete: This deletes the corresponding User account.

Redeem On-demand Accounts

For Usage-time accounts, when the remaining quota is insufficient or if they are running out of quota, users can use the redeem function to extend their quota. After the user has bought a new account, they just need to click the **Redeem** button in the login success page, input the new account **Username** and **Password** and then click **Enter**. This new account's quota will be extended to the original account. However, the Redeem function can only be used with the same billing type, i.e. Volume accounts can only be redeemed with another Volume account and so on.



Note: The maximum quota is "364dys 23hrs 59mins 59secs" even after redemption. If the redeemed amount exceeds this number, the system will automatically reject the redemption process.

Note: Duration-time and Hotel Cut-off type do not support redemption function.

Free Authentication



System Users Network Utilities Status

Authentication Black List Group Policy Schedule Firewall QoS Specific Route Privilege Additional Control Operator

[Main Menu](#) > [Users](#) > [Authentication](#) > FREE Authentication

Authentication Server - FREE	
Group	Group 1 ▾
Trial Account	☐ Enable ☒ Disable

Apply Cancel

When the Free Authentication option is **Enabled**, users will have an option of logging in with an email address without authentication. This can be activated under Service Zone Settings configurations. The constraints can be set specifically with the mapped Group profile. MAC addresses will be checked to avoid malicious use of free access.



System Users Network Utilities Status

Authentication Black List Group Policy Schedule Firewall QoS Specific Route Privilege Additional Control Operator

[Main Menu](#) > [Users](#) > [Authentication](#) > FREE Authentication

Authentication Server - FREE	
Group	Group 1 ▾
Trial Account	☒ Enable ☐ Disable
Usage Time	2 hour(s) 0 minute(s)
Refresh Time	12 hour(s)(1~999 three digits)
Trial Account List	View

Apply Cancel

When Trial Account is Enabled, the Administrator can choose to set the Usage Time and Refresh Time. The server remembers the MAC address of the user. Hence the user can only get a new Free authentication account after the refresh time has been reached

User Login

Default Authentication

There are different types of authentication databases (LOCAL, RADIUS and ONDEMAND) that are supported by the system. But authentication can only be set in the Public Zone.

A suffix is used to inform the system which authentication option is to be used for authenticating an account (e.g. Bob@local or Tim@radius1 etc.) when multiple options are concurrently in use. One of the authentication options can be assigned as default. For authentication assigned as default, the suffix can be omitted. For example, if "local" is the suffix of the default option, then user with username Bob can login as "Bob" without the need to type in "Bob@local".

Authentication Options	Auth Option	Auth Database	Postfix	Default	Enable
	Server 1	LOCAL	local	☒	☒
	Server 2	RADIUS	radius1	☐	☒
	Server 3	RADIUS	radius2	☐	☒
	On-demand User	ONDEMAND	ondemand	☐	☒
	FREE	FREE	N/A	☐	☐

Login with Suffix

For each authentication option, set a suffix that is easy to distinguish (e.g. Local) users according to different authentication servers. The acceptable characters are numbers (0~9), alphabet (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

Beside the users managed by Default Authentication, all the other ones with different servers should log into the system with usernames containing suffixes to identify which authentication option they belong to.

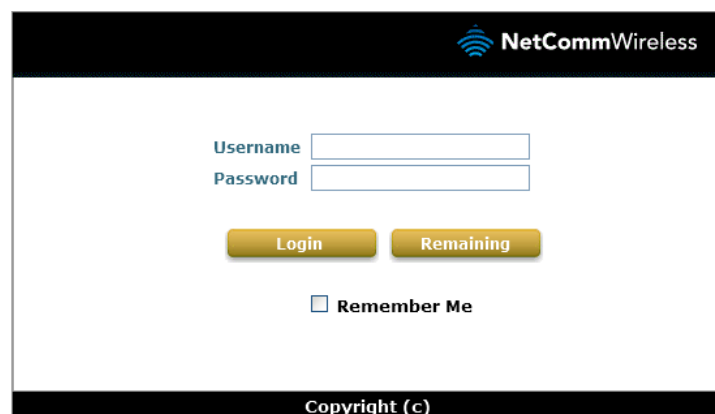
The suffix can be set for each Authentication database by clicking the Auth Option.

An Example of User Login

Normally, users will be authenticated before they get network access through gateway. This section presents the basic authentication process of end users. Please make sure that the gateway is configured properly and the network-related settings are done.

1. Connect a client PC to Public Zone of gateway. Open an Internet browser and try to connect to any website (in this example, we try to connect to www.google.com).

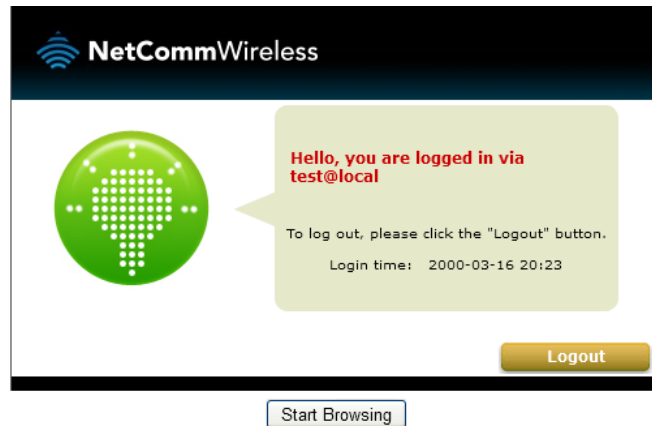
The default user login page will appear in the browser.



The image shows a screenshot of the NetCommWireless user login page. At the top, there is a black header with the NetCommWireless logo and name. Below the header, the page has a white background. It features two input fields: 'Username' and 'Password'. Below these fields are two yellow buttons: 'Login' and 'Remaining'. Under the buttons is a checkbox labeled 'Remember Me'. At the bottom of the page, there is a black footer with the text 'Copyright (c)'.

2. Enter the username and password (for example, we use a local user account: test@local here) and then click **Login**. If the Remember Me checkbox is checked, the browser will store the username and the password on the current computer in order to automatically login to the system at the next login. Then, click the **Login** button.

The **Remaining** button on the **User Login Page** is for on-demand users only; this is where they can check their Remaining quota.



The **Login Success Page** indicates that you are connected to the network and the Internet now.

Banning Users

Black List

To configure a Black List, go to **Users >> Black List**.

The administrator can add, delete, or edit the black list for user access control. User accounts that appear on the black list will be denied of network access. The administrator can use the pull-down menu to select the desired black list.

Black List Settings		
Select Black List	1:Blacklist1 ▼	
Name	Blacklist1	
User	Remark	Del All

(Total:0/20) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page ▼ (Page:1/1) Row per Page: 10 ▼

[Add User\(s\)](#)

Select Black List: There are 5 black list profiles available for use.

Name: Set the black list name and it will show on the pull-down menu above.

Add User(s): Click the **Add User(s)** button to add users to the selected black list.

Adding User(s) to Blacklist1		
No.	Username	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

After entering the username in the **"Username"** field and the related information in the **"Remark"** blank (not required), click **Apply** to add the user.

If a user needs to be removed from the black list, click the user's **"Delete"** button and or use click **Del All** button to remove all users from the black list.

Black List Settings		
Select Black List	1:Blacklist1 ▼	
Name	Blacklist1	
User	Remark	Del All
blackuser		Delete

(Total:1/20) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page 1 ▼ (Page:1/1) Row per Page: 10 ▼

[Add User\(s\)](#)

After the Black List editing is completed. You can select the Black List in each Authentication Server to make the list effective.

Group

To configure Group, go to: **Users >> Group**.

Users on the gateway can be classified into different groups, which can be assigned different Policies and Schedules. The gateway supports up to 5 user Groups.

Group Configuration - Group 1			
Select Group	Group 1 ▼		
Group Name	Group 1		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	Enabled	Time Span 1	Time Span 2
		Schedule 1 ▼	Schedule 1 ▼
Service Zone : Private	☒	Policy 1 ▼	Policy 1 ▼
Service Zone : Public	☒	Policy 1 ▼	Policy 1 ▼

When the type of authentication database is **RADIUS**, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Group will be mapped to a user of a RADIUS class attribute.

Policy

To configure Policy, go to: **Users >> Policy**.

The gateway supports multiple Policies, including one **Global Policy** and 5 individual **Policies**.

Global Policy is the system's universal policy and is applied to all clients unless the clients are bound by another policy. Individual Policy can be defined and applied to a different authentication server. A client logging in with this authentication server will be bound by the corresponding Policy. If no policy is applied to the authentication server, its users will be governed by the Global Policy.

Global Policy

Global policy is the system's universal policy containing the **Firewall Profile**, **Specific Routes Profile (IPv4/IPv6)**, and **Privilege Profile**, which will be applied to all users unless the user has been regulated by another individual Policy.

Policy Configuration - Global Policy	
Select Policy	Global ▼
Firewall Profile	<button>Configure</button>
Specific Route Profile	<button>Configure</button>
Specific IPv6 Route Profile	<button>Configure</button>
Privilege Profile	<button>Configure</button>

Select Policy: Select a desired policy profile to configure.

Firewall Profile: Global policy and policy 1 ~ 5 all have a firewall service list and a set of firewall profiles which is composed of firewall rules.

Specific Route Profile: When Specific Routes are configured here, all clients applied with this policy will access the specific destination through these gateway settings.

Specific IPv6 Route Profile: The routing rules to be applied to users using IPv6 under this policy may be configured here.

Privilege Profile: Enable or Disable Users' privilege to change password. Administrator can set the maximum sessions per user here.

Policy 1 ~ Policy 5

Beside **Global Policy**, **Policy 1** to **Policy 5**, each consists of access control profiles that can be respectively configured and applied to a certain authentication server or user.

Policy Configuration - Policy 1	
Select Policy	Policy 1 Configure
Firewall Profile	Firewall 1 Configure
QoS Profile	Traffic 1 Configure
Specific Route Profile	Specific Route 1 Configure
Privilege Profile	Privilege 1 Configure

Select Policy: Select a desired policy profile to configure.

Firewall Profile: Each Policy has a firewall service list and a set of firewall profiles consisting of firewall rules.

QoS Profile: QoS profile defines the traffic class for the users governed by this Policy.

Specific Route Profile: The default gateway of a desired IP address can be defined in a policy. When Specific Routes are configured here, all clients applied with this policy will access the specific destination through these gateway settings.

Privilege Profile: Enable or Disable Users' privilege to change password. Administrator can set the maximum sessions per user here.

Schedule

To configure a schedule profile, click **User >> Schedule** to enter the configuration page. The configuration page shows the **Permitted Login Hours** list. This function is used to limit the time when clients can log in. Select the desired time-slot checkboxes and click **Apply** to save the settings. These settings will become effective immediately after clicking **Apply**. Administrator can also choose to **Enable** or **Disable** Auto logout when a user exceeds the permitted login hours. Up to 5 profiles can be configured.

Schedule Configuration	
Auto logout station by system	☐ Enable ☒ Disable
Apply Cancel	

Permitted Login Hours - Profile 1							
Select Profile	Profile 1 Configure						
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
00:00~00:59	☒	☒	☒	☒	☒	☒	☒
01:00~01:59	☒	☒	☒	☒	☒	☒	☒
02:00~02:59	☒	☒	☒	☒	☒	☒	☒
03:00~03:59	☒	☒	☒	☒	☒	☒	☒
04:00~04:59	☒	☒	☒	☒	☒	☒	☒
05:00~05:59	☒	☒	☒	☒	☒	☒	☒
06:00~06:59	☒	☒	☒	☒	☒	☒	☒

Firewall

To configure the firewall, Click **User >> Firewall**. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules. Up to 5 profiles can be configured.

Firewall Configuration - Profile 1	
Select Profile	Profile 1 ▼
Predefined and Custom Service Protocols	<button>Configure</button>
User Firewall Rules	<button>Configure</button>
User Firewall Rules (IPv6)	<button>Configure</button>

Predefined and Custom Service Protocols

Predefined and Custom Service Protocols: There are predefined service protocols available for firewall rule editing.

Firewall Profile 1 - Service Protocols List			
No.	Name	Description	Select All
0	ALL	ALL	☐
1	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
2	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL ICMP	ICMP; Type: Any, Code: Any	☐
4	FTP	TCP/UDP; Destination Port: 20;21	☐
5	HTTP	TCP/UDP; Destination Port: 80	☐
6	HTTPS	TCP/UDP; Destination Port: 443	☐
7	POP3	TCP; Destination Port: 110	☐
8	SMTP	TCP; Destination Port: 25	☐
9	DHCP	UDP; Destination Port: 67;68	☐
10	DNS	TCP/UDP; Destination Port: 53	☐

The administrator is able to add new custom service protocols by clicking **Add**, and delete the added protocols individually or with **Select All** followed by **Delete** operation.

Caution: The Predefined Service Protocols cannot be deleted.

Click **Add** to add a custom service protocol. The **Protocol Type** can be defined from a list of service by protocols (TCP/UDP/ICMP/IP); and then define the **Source Port** (range) and **Destination Port** (range); click **Apply** to save this protocol.

Add Service Protocol	
Name	
Protocol Type	TCP ▼
Source Port	1 ~ 65535
Destination Port	1 ~ 65535

Apply Cancel

If the Protocol Type is ICMP, the Type and Code must be defined.

Add Service Protocol			
Name			
Protocol Type	ICMP ▾		
Type		Code	

If the Protocol Type is IP, the Protocol Number needs to be defined.

Add Service Protocol	
Name	
Protocol Type	IP ▾
Protocol Number	

User Firewall Rules

After the custom protocol is defined(or just use the **Predefined Service Protocols**), you will need to enable the **Firewall Rule** to apply these protocols. Firewall Rules for IPv6 is also supported.

Firewall Rules: Click **Rule No.** to edit individual rules and click **Apply** to save the settings. The rule status will be shown on the list. Check the **"Active"** checkbox and click **Apply** to enable the rule.

Rule No.1 has the highest priority; Rule No.2 has the second highest priority and so on. Each firewall rule is defined by Source, Destination and Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to **Always**, **Recurring** or **One Time**.

Firewall Profile 1 - Firewall Rules									Create a New Rule
No.	Active	Action	Rule Name	Source	Destination	Service	Schedule	Operation	
				Source Interface	Destination Interface				
									(Total:0/10) First Prev Next Last Go to Page ▾ (Page:1/1) Row per Page: 20 ▾
									Create a New Rule
									Apply Cancel

Selecting the Filter Rule Number 1 as an example:

Policy 1 - Edit Filter Rule			
Rule Number	1		
Rule Name			
Source		Destination	
Interface/Zone	ALL ▾	Interface/Zone	ALL ▾
IP Address ▾	0.0.0.0	IP Address ▾	0.0.0.0
Subnet Mask	0.0.0.0 (/0) ▾	Subnet Mask	0.0.0.0 (/0) ▾
MAC Address			
Service Protocol	ALL ▾		
Schedule	☒ Always ☐ Recurring ☐ One Time		
Action for Matched Packets	☒ Block ☐ Pass		

Rule Number: This is the rule selected “1”. Rule No. 1 has the highest priority; rule No. 2 has the second highest priority, and so on.

Rule Name: The rule name can be changed here.

Source/Destination – Interface/Zone: There are choices of **ALL**, **WAN**, **Public** and **Private** to be applied for the traffic interface.

Source/Destination – IP Address/Domain Name: Enter the source and destination IP addresses. Domain Name filtering is supported but Domain Host filtering is not.

Source/Destination – Subnet Mask: Select the source and destination subnet masks.

Source- MAC Address: The MAC Address of the source IP address. This is for specific MAC address filtering.

Service Protocol: These are defined protocols on the **service protocols list** to be selected.

Schedule: When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time**. **Recurring** is set with the hours within a week.

Action for Matched Packets: There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

QoS Profile

Up to 5 QoS profiles can be configured for certain applications or users that need stable bandwidth or traffic priority. Bandwidth Control can only be Enabled when Bandwidth limits on WAN has been Enabled.

Traffic Configuration - Profile 1	
Select Profile	Profile 1 ▼
Traffic Class	IPv4 IPv6
Bandwidth Control	☒ Enable ☐ Disable
Group Total Downlink	0 Mbps ▼ *(Unlimit: 0, Range: 1-999)
Individual Maximum Downlink	0 Mbps ▼ *(Unlimit: 0, Range: 1-999)
Individual Request Downlink	0 Mbps ▼ *(Unlimit: 0, Range: 1-999)
Group Total Uplink	0 Mbps ▼ *(Unlimit: 0, Range: 1-999)
Individual Maximum Uplink	0 Mbps ▼ *(Unlimit: 0, Range: 1-999)
Individual Request Uplink	0 Mbps ▼ *(Unlimit: 0, Range: 1-999)

Traffic Class: Traffic Class can be chosen for users on IPv4 or IPv6. Default DSCP (Differentiated Services Code Point) can be added and edited to determine traffic class. Default DSCP includes: Network Control 0x30, Telephony 0x2E, Signaling 0x28, Multi-media Conferencing 0x26, Real-Time Interactive 0x20, Multi-media Streaming 0x1A, Broadcast Video 0x18, Low-latency Data 0x12, OAM 0x10, High-Throughput Data 0x0A, Standard 0x00, Low Priority Data 0x08.

Bandwidth Control: Enable or Disable the capability to determine the following parameters.

Group Total Downlink: Defines the maximum bandwidth allowed to be shared by clients.

Individual Maximum Downlink: Defines the maximum downlink bandwidth allowed for an individual client. The Individual Maximum Downlink cannot exceed the value of Group Total Downlink.

Individual Request Downlink: Defines the guaranteed minimum downlink bandwidth allowed for an individual client. The Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.

Group Total Uplink: Defines the maximum uplink bandwidth allowed to be shared by clients.

Individual Maximum Uplink: Defines the maximum uplink bandwidth allowed for an individual client. The Individual Maximum Uplink cannot exceed the value of Group Total Uplink.

Individual Request Uplink: Defines the guaranteed minimum bandwidth allowed for an individual client. The Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

Routing

To configure routes, click **User >> Specific Route** for the **Specific Route Profile**, the 'Specific Route Profile' list appears.

Specific Route

Specific Route Profile: The Specific Default Route is used to control clients to access some specific IP segment by the specified gateway. Specific Routing can be set up for the Global Policy and up to 5 profiles can be configured.

Global Policy - Specific Routes			
Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32) ▼	
2		255.255.255.255 (/32) ▼	
3		255.255.255.255 (/32) ▼	
4		255.255.255.255 (/32) ▼	

Specific Routes - Profile 1			
Select Profile		Profile 1 ▼	
Enable ☐		Default Gateway: IP Address ▼	
Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32) ▼	
2		255.255.255.255 (/32) ▼	
3		255.255.255.255 (/32) ▼	
4		255.255.255.255 (/32) ▼	
5		255.255.255.255 (/32) ▼	
6		255.255.255.255 (/32) ▼	
7		255.255.255.255 (/32) ▼	
8		255.255.255.255 (/32) ▼	

Destination / IP Address: The destination network address or IP address of the destination host. Please note that, if applicable, the system will calculate and display the appropriate value based on the combination of Network/IP Address and Subnet Mask that have just been entered and applied.

Destination / Subnet Netmask: The subnet mask of the destination network. Select 255.255.255.255(/32) if the destination is a single host.

Gateway / IP Address: The IP address of the gateway or next router to the destination.

Default Gateway

Default Gateway: The default gateway of a desired IP address can be defined in each Policy except Global Policy. When Specific Default Route is enabled, all clients applied with this Policy will access the Internet through this default gateway.

Specific Routes - Profile 1	
Select Profile	Profile 1 ▾
Enable ☒	Default Gateway: IP Address ▾

Enable: Check the **Enable** box to activate this function or uncheck to deactivate it.

Default Gateway IP Address: You may need to fill in the IP address of the default gateway.

User Privilege

Administrator can choose to allow users to change their Password. And to prevent ill-behaved clients or malicious software from taking up the system's connection resources, the administrator can restrict the number of concurrent sessions that a user can establish.

Privilege Configuration - Profile 1	
Select Profile	Profile 1 ▾
Change Password Privilege	☐ Enable ☒ Disable
Maximum Concurrent Sessions	Unlimited ▾ (sessions per user)

The maximum number of concurrent sessions including TCP and UDP for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones. This can also be specified in the other policies to apply to the authenticated users.

When a user reaches the defined session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350, 500, 750 and 1000), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a SYSLOG server.

Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

Accessing the Network without Authentication

DMZ

To configure DMZ, go to: **Network >> Network Address Translation >> DMZ (Demilitarized Zone)**.



The screenshot shows the 'Network Address Translation' configuration page. The 'DMZ (Demilitarized Zone)' option is highlighted with a red box, and its 'Configure' button is also highlighted. Other options include 'Public Accessible Server' and 'Port and IP Forwarding', each with a 'Configure' button.

There are 40 sets of static Internal IP Address and External IP Address available. Enter **Internal** and **External** IP Address as a set. After the setup, accessing the External IP address listed in DMZ will be mapped to accessing the corresponding Internal IP Address. These settings will become effective immediately after clicking the **Apply** button. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN) that will change dynamically if WAN Interface is Dynamic. When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with WAN interface.

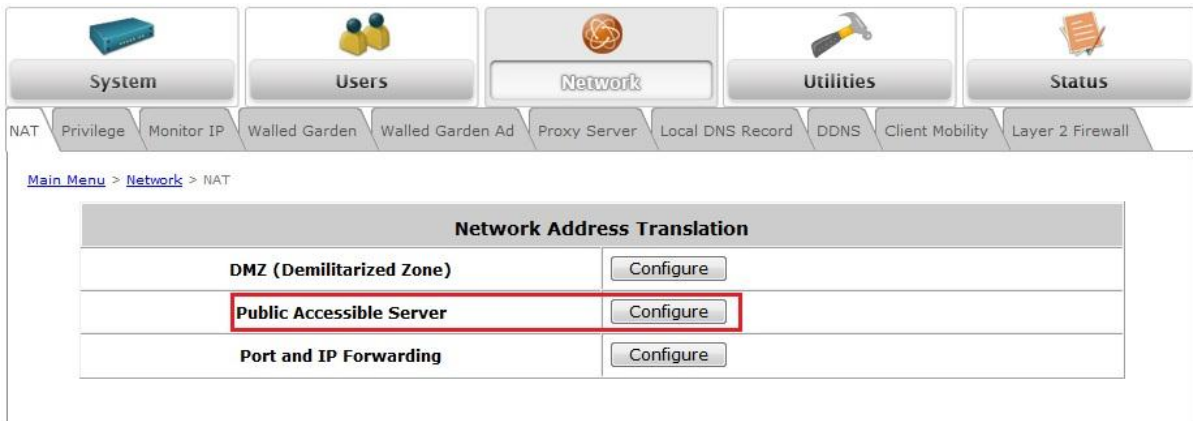
Automatic WAN IP Assignment				
Enable	External IP Address	External Interface	Internal IP Address	Remark
☐	10.16.29.79	WAN		

Static Assignments				
No.	External IP Address	External Interface	Internal IP Address	Remark
1		WAN ▾		
2		WAN ▾		
3		WAN ▾		
4		WAN ▾		
5		WAN ▾		
6		WAN ▾		
7		WAN ▾		
8		WAN ▾		
9		WAN ▾		
10		WAN ▾		

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/4) Row per Page:

Virtual Server

To configure Virtual Server, go to: **Network >> Network Address Translation >> Public Accessible Server**



The screenshot shows the NetComm Wireless web interface. At the top, there are five main tabs: System, Users, Network, Utilities, and Status. Below these, there are sub-tabs for NAT, Privilege, Monitor IP, Walled Garden, Walled Garden Ad, Proxy Server, Local DNS Record, DDNS, Client Mobility, and Layer 2 Firewall. The 'Network' tab is selected, and the 'NAT' sub-tab is active. The 'Main Menu > Network > NAT' breadcrumb is visible. The 'Network Address Translation' section contains three options: 'DMZ (Demilitarized Zone)', 'Public Accessible Server' (highlighted with a red box), and 'Port and IP Forwarding'. Each option has a 'Configure' button next to it.

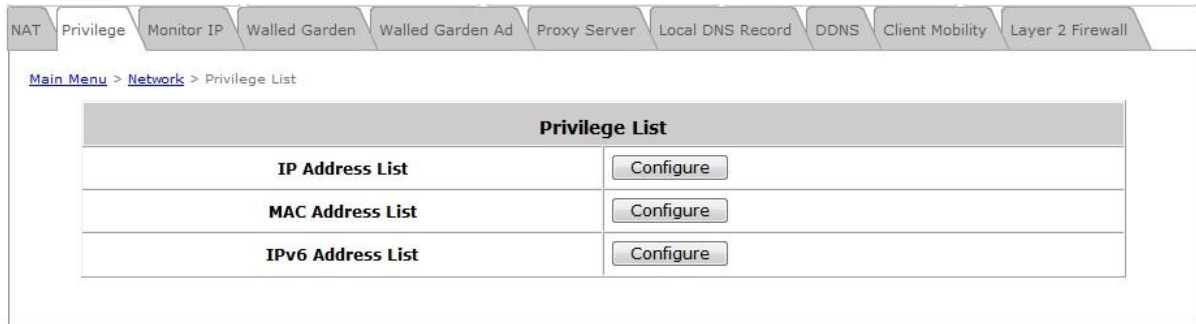
This function allows the administrator to set 40 virtual servers at most, so that client devices outside the managed network can access these servers within the managed network. Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general. Enter the “**External Service Port**”, “**Local Server IP Address**” and “**Local Server Port**”. Select “**TCP**” or “**UDP**” for the service type. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the **Apply** button.

Public Accessible Server						
No.	External Service Port	Local Server IP Address	Local Server Port	Type	Enable	Remark
1				☒ TCP ☐ UDP	☐	
2				☒ TCP ☐ UDP	☐	
3				☒ TCP ☐ UDP	☐	
4				☒ TCP ☐ UDP	☐	
5				☒ TCP ☐ UDP	☐	
6				☒ TCP ☐ UDP	☐	
7				☒ TCP ☐ UDP	☐	
8				☒ TCP ☐ UDP	☐	
9				☒ TCP ☐ UDP	☐	
10				☒ TCP ☐ UDP	☐	

Privilege List

To configure the Privilege List, go to: **Network >> Privilege**

Setup the **Privilege IP Address List**, **Privilege MAC Address List** and the **Privilege IPv6 Address List**. The clients accessing the internet via IP addresses and/or networking devices on the list can access the network without any authentication.



Privilege List

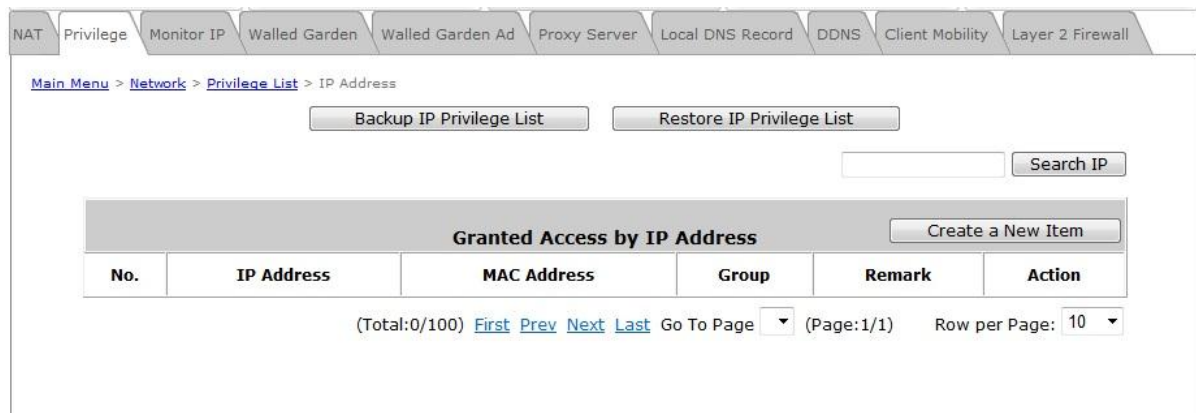
IP Address List	Configure
MAC Address List	Configure
IPv6 Address List	Configure

Privilege IP

Privilege IP Address List

To configure Privilege IP Address List, go to: **Network >> Privilege >> IP Address List**.

If there are workstations inside the managed network that need to access the network without authentication, enter the IP addresses of these workstations in "Granted Access by IP Address". The "Remark" field is not necessary but is convenient for keeping track. The gateway allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.



Granted Access by IP Address

No.	IP Address	MAC Address	Group	Remark	Action
(Total:0/100) First Prev Next Last Go To Page (Page:1/1) Row per Page: 10					

Caution: Permitting specific IP addresses to have network access rights without going through standard authentication process under Public zone may cause security problems.

Privilege MAC

Privilege MAC Address List

In addition to the Privilege IP List, MAC address List allows the MAC address of the workstations that need to access the network without authentication to be set in "Granted Access by MAC Address". The gateway allows 100 privileged MAC addresses at most. When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (optional). These settings will be effective immediately after clicking **Apply**.

Granted Access by MAC Address		
No.	MAC Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total: 100) [First](#) [Prev](#) [Next](#) [Last](#)

Caution: Permitting specific MAC addresses to have network access rights without going through standard authentication process under Public zone may cause security problems.

Privilege IPv6

Privilege IPv6 Address List

In addition to the Privilege IP List, MAC address List, the privilege IPv6 List allows the IPv6 address of the workstations that need to access the network without authentication to be set in "Granted Access by IPv6 Address". The gateway allows 100 privileged IPv6 addresses at most. When manually creating the list, enter the IPv6 address (the format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx) as well as the remark (optional). These settings will be effective immediately after clicking **Apply**.

Disable Authentication in Public Zone

To disable Authentication in Public Zone, go to: **System >> Service Zones**, click **Configure** in **Public Zone**.

Service Zone Settings						
Service Zone Name	Applied Policy	IP Address	Network Alias	DHCP Pool	LAN Port Mapping	Details
	Default Authen Option	IPv6 Address			Status	
Private	Policy 1	192.168.1.254	N/A	192.168.1.1 ~ 192.168.1.100		Configure
	Disabled	N/A			Enabled	
Public	Policy 1	172.21.0.254	N/A	172.21.0.1 ~ 172.21.0.100		Configure
	Server 1	N/A			Enabled	

Authentication Settings					
Authentication Required For the Zone	☒ Enable ☐ Disable ☐ Suspend				
WISPr Configuration	Configure				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enable
	Server 1	LOCAL	local	☒	☒
	Server 2	RADIUS	radius1	☐	☒
	Server 3	RADIUS	radius2	☐	☒
	On-demand User	ONDEMAND	ondemand	☐	☒
	FREE	FREE	N/A	☐	☐

Authentication Required For the Zone: When it is disabled, users will not need to authenticate before they get access to the network within Public Zone.

User Login and Logout

Before Login

Login with SSL

To configure HTTPS, go to: **System >> General**.

HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sub-layer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

The **HTTPS Protected Login** function makes the client's login more secure. Enable it to activate https (encryption) or disable it to activate http (non encryption) login page.

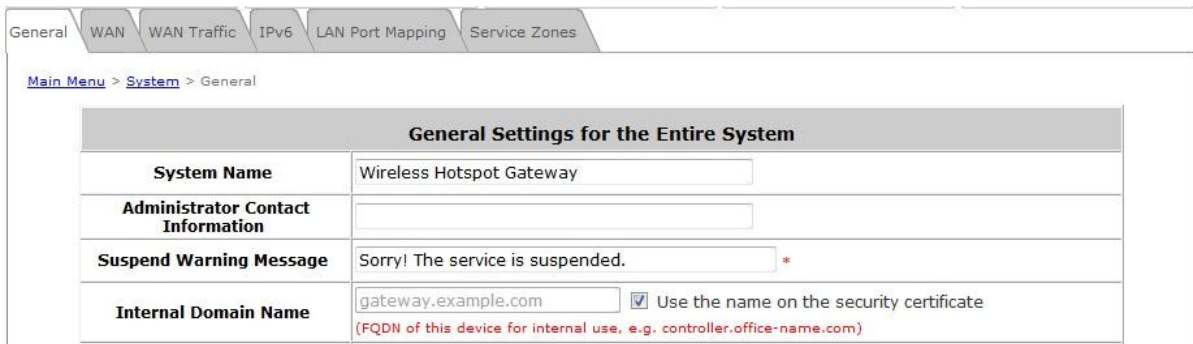
General Settings for the Entire System	
System Name	Wireless Hotspot Gateway
Administrator Contact Information	
Suspend Warning Message	Sorry! The service is suspended. *
Internal Domain Name	gateway.example.com ☒ Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Disclaimer Page	☐ Enable ☒ Disable
Portal URL	☒ Specific ☐ Original ☐ None http://www.google.com *(e.g. http://www.example.com) Browser ID(User Agent) IEMobile/7.0.XBLWP7 (e.g. IEMobile/7.0.XBLWP7, separate by comma)
UAM Filter	Configure
User Log Access IP Address	(e.g. 192.168.2.1)
Management IP Address List	Configure
SNMP	☒ Enable ☐ Disable Configure
HTTPS Certificate	Default CERT ▾
HTTPS Protected Login	☐ Enable ☒ Disable

Internal Domain Name with Certificate

To configure Internal Domain Name, go to: **System >> General**.

Internal Domain Name is the domain name of the gateway seen on client machines connected under zone. It must conform to FQDN (Fully-Qualified Domain Name) standard. A user on client machine can use this domain name to access the gateway instead of its IP address.

In addition, when “**Use the name on the security certificate**” option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.



The screenshot shows the 'General Settings for the Entire System' configuration page. The 'Internal Domain Name' field is set to 'gateway.example.com'. The checkbox 'Use the name on the security certificate' is checked. Below the checkbox, a red note states: '(FQDN of this device for internal use, e.g. controller.office-name.com)'.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway
Administrator Contact Information	
Suspend Warning Message	Sorry! The service is suspended. *
Internal Domain Name	gateway.example.com ☒ Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)

To Configure Certificate, go to: **Utilities >> Certificate** and choose Upload Certificate from the scroll down menu.

Certificate: A data record used for authenticating network entities such as a server or a client. A certificate contains X.509 information pieces about its owner (called the subject) and the signing Certificate Authority (called the issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates. You can apply for a SSL certificate at CAs such as VeriSign.

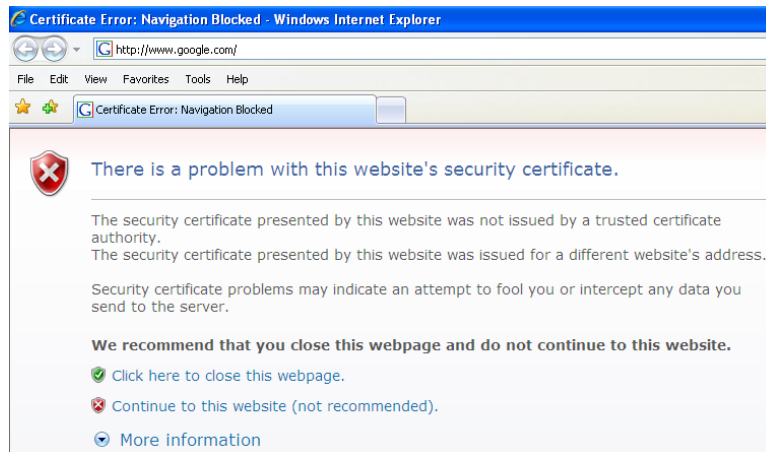
If you already have a SSL Certificate, please Click **Browse** to select the file and upload it. Click **Apply** to complete the upload process. If you do not have a valid SSL Certificate, use the system default certificate.



The screenshot shows the 'Certificate Utility' configuration page. The 'Upload Certificate' dropdown menu is selected. The 'Private Key' and 'Certificate' fields are empty, each with a 'Browse...' button. The 'Certification Path Verification' is set to 'Disable'.

Certificate Utility	
Upload Certificate ▼	
Upload Certificate	
Private Key	Browse...
Certificate	Browse...
Certification Path Verification	☐ Enable ☒ Disable

Without a valid certificate, users may encounter the following warning when trying to open the login page.



Click "Continue to this website" to access the user login page.

Walled Garden

To configure Walled Garden, go to: **Network >> Walled Garden**.

This function provides certain free services for users to access the websites listed here before login and authentication. Up to 20 addresses or domain names of the websites can be defined on this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the **IP Address** or **Domain Name** (of the website) on the list and click **Apply** to save the settings.

Add Walled Garden List				
No.	Active	Domain Name/IP Address	Service Zone	Remark
1	☐		All ▼	
2	☐		All ▼	
3	☐		All ▼	
4	☐		All ▼	
5	☐		All ▼	
6	☐		All ▼	
7	☐		All ▼	
8	☐		All ▼	
9	☐		All ▼	
10	☐		All ▼	

Walled Garden AD

To configure Walled Garden AD List, go to: **Network >> Walled Garden AD**.

This function provides advertisement links to web pages for users to access free of charge before login and authentication. Advertisement hyperlinks are displayed on the user's login page. Clients who click on it will be redirected to the listed advertisement websites.

Walled Garden Ad List				
Item	URL	Topic	Edit	Display
	Description			
1			<button>Edit</button>	☐
2			<button>Edit</button>	☐
3			<button>Edit</button>	☐
4			<button>Edit</button>	☐
5			<button>Edit</button>	☐
6			<button>Edit</button>	☐
7			<button>Edit</button>	☐
8			<button>Edit</button>	☐
9			<button>Edit</button>	☐
10			<button>Edit</button>	☐

Enter all items or make changes by clicking the **Edit** button, click **Apply**, the items will be added and shown on the list.

URL: Enter the URL of the advertisement website.

Topic: Enter the content of the hyperlink, for instance if you enter Google in this field, on the user login page a hyperlink of [Google](#) will be displayed.

Description: Any additional message for administrator's reference.

Display: Choose **Display** to display advertisement hyperlinks on the login pages.

After Login

Portal URL after successful login

To configure Portal URL after a successful user login, go to: **System >> General**.

When this function is enabled, enter the URL of a Web server as the Portal page. Once logged in successfully, users will be directed to this URL, such as <http://www.google.com>, regardless of the original homepage set in their browsers.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway
Administrator Contact Information	
Suspend Warning Message	Sorry! The service is suspended. *
Internal Domain Name	gateway.example.com ☒ Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Disclaimer Page	☐ Enable ☒ Disable
Portal URL	☒ Specific ☐ Original ☐ None http://www.google.com *(e.g. http://www.example.com) Browser ID(User Agent) IEMobile/7.0.XBLWP7 (e.g. IEMobile/7.0.XBLWP7, separate by comma)

When this function is set to **None**, after users logged in successfully, users will be directed to the original homepage set in their browsers.

Idle Timer

To configure Idle Timer, go to: **Users >> Additional Control**.

If a user has idled with no network activities, the system will automatically kick the user out. The logout timer can be set between 1~1440 minutes, and the default idle time is 10 minutes.

Additional Control		
User Session Control	Idle Timeout (minutes)	10 *(1-1440)
	Interval for Idle Traffic Detection (seconds)	60 *(1-600)
	Threshold for Idle Traffic Detection (bytes)	0 *(0-1048576, 0 is Disabled)
	Idle Timeout Check Direction	☐ Uplink ☒ Uplink & Downlink
	Multiple Login	☐ Enable (This function is not applicable to on-demand accounts.)
	Charge Traffic to/from Hosts in Walled Garden List	☐ Enable ☒ Disable
	Kick out users when their IPs are changed	☐ Enable ☒ Disable

Multiple Login

To configure Multiple Login, go to: **Users >> Additional Control**.

When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users.)

Additional Control			
User Session Control	Idle Timeout (minutes)	10	*(1-1440)
	Interval for Idle Traffic Detection (seconds)	60	*(1-600)
	Threshold for Idle Traffic Detection (bytes)	0	*(0-1048576, 0 is Disabled)
	Idle Timeout Check Direction	☐ Uplink ☒ Uplink & Downlink	
	Multiple Login	☒ Enable (This function is not applicable to on-demand accounts.)	
	Charge Traffic to/from Hosts in Walled Garden List	☐ Enable ☒ Disable	
	Kick out users when their IPs are changed	☐ Enable ☒ Disable	

Networking Features of a Gateway

IP Plug and Play

To configure IP Plug and Play, go to: **Network >> Client Mobility**.

The gateway supports IP PNP function. A user can log in and access network with any IP address setting. This function is disabled in default settings.

Client Mobility	
IP PNP	☐ Enable ☒ Disable

When **IP PNP** is enabled, at the user end, a static IP address can be used to connect to the system. Regardless of what the IP address at the user end is using, authentication can still be performed through the gateway.

Note: To apply for free Dynamic DNS service, you may go to <http://www.dyndns.com/services/dns/dyndns/howto.html>

Port and IP Forwarding

To configure Port and IP Forwarding, go to: **Network >> NAT >> Port and IP Forwarding**.

This function allows the administrator to set at most 40 sets of IP addresses for redirection purposes. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the "IP Address" and "Port" of **Destination**, and the "IP Address" and "Port" of **Translated to Destination**. Select "TCP" or "UDP" for the service's type. These settings will become effective immediately after clicking **Apply**.

Port and IP Forwarding						
No.	Destination		Translated to Destination		Type	Remark
	IP Address	Port	IP Address	Port		
1					☒ TCP ☐ UDP	
2					☒ TCP ☐ UDP	
3					☒ TCP ☐ UDP	
4					☒ TCP ☐ UDP	
5					☒ TCP ☐ UDP	
6					☒ TCP ☐ UDP	
7					☒ TCP ☐ UDP	
8					☒ TCP ☐ UDP	
9					☒ TCP ☐ UDP	
10					☒ TCP ☐ UDP	

System Management and Utilities

System Time

To configure System Time, go to: **System >> General**.

NTP (Network Time Protocol) communication protocol can be used to synchronize the system time with remote time server. Please specify the local time zone and the IP address of at least one NTP server for adjusting the time automatically (Universal Time is Greenwich Mean Time, GMT).

Manual setup is another option to set up the system time, if you choose to set up the system time manually, please enter the Year, Month, Day, the current time and click Apply to activate the changes.

Time	System Time : 2013/08/20 16:41:23	
	Time Zone :	
	(GMT+10:00)Canberra,Melbourne,Sydney	
	☒ NTP	
	NTP Server 1:	0.netcomm.pool.ntp *(e.g. tock.usno.navy.mil)
	NTP Server 2:	1.netcomm.pool.ntp
	☐ Manually set up	

NTP Server Mode: When Enabled, Access Points and devices in the Local Area Network of the gateway would be able to use the gateway as a NTP Server for time reference.

Note: When system can not sync the time with NTP server, all clients will not be allowed to log in to system and On-demand accounts cannot be created.

Management IP Address List

To configure the Management IP Address List, go to: **System >> General**.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway
Administrator Contact Information	
Suspend Warning Message	Sorry! The service is suspended. *
Internal Domain Name	gateway.example.com ☒ Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Disclaimer Page	☐ Enable ☒ Disable
Portal URL	☒ Specific ☐ Original ☐ None http://www.google.com *(e.g. http://www.example.com) Browser ID(User Agent) IEMobile/7.0.XBLWP7 (e.g. IEMobile/7.0.XBLWP7, separate by comma)
UAM Filter	Configure
User Log Access IP Address	(e.g. 192.168.2.1)
Management IP Address List	Configure

Only PCs within the Management IP range on the list are allowed to access the system's web management interface. For example, 10.2.3.0/24 means that as long as an administrator is using a computer with the IP address range of 10.2.3.0/24, he or she can access the web management page. Another example is 10.0.0.3: if an administrator is using a computer with the IP address of 10.0.0.3, he or she can access the web management page.

Management IP Address List					
No.	Active	IP Address/Segment	No.	Active	IP Address/Segment
1	☒	0.0.0.0/0.0.0.0	2	☐	
3	☐		4	☐	
5	☐		6	☐	
7	☐		8	☐	
9	☐		10	☐	
11	☐		12	☐	
13	☐		14	☐	
15	☐		16	☐	
17	☐		18	☐	
19	☐		20	☐	

The default value is "0.0.0.0/0.0.0.0". It means that the WMI can be accessed by any IP address, for security consideration; please change this value before the system provides service.

IP Address for Accessing User Log

To configure User Log Access IP History, go to: **System >> General**.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway
Administrator Contact Information	
Suspend Warning Message	Sorry! The service is suspended. *
Internal Domain Name	gateway.example.com ☒ Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Disclaimer Page	☐ Enable ☒ Disable
Portal URL	☒ Specific ☐ Original ☐ None http://www.google.com * (e.g. http://www.example.com) Browser ID (User Agent) IEMobile/7.0.XBLWP7 (e.g. IEMobile/7.0.XBLWP7, separate by comma)
UAM Filter	Configure
User Log Access IP Address	(e.g. 192.168.2.1)
Management IP Address List	Configure

Specify an IP address of the administrator's computer or a billing system to get billing history information of the gateway with the predefined URLs. The file name format is "yyyy-mm-dd" such as the following:

Traffic History : <https://10.2.3.213/status/history/2012-02-10>

On-demand History: <https://10.2.3.213/status/odhistory/2012-07-10>

SNMP

To configure SNMP, go to: **System >> General**. The gateway supports SNMP v1/v2c.

If this function is enabled, the SNMP Management IP and the Community string can be assigned for SNMP management applications to access the system.

General Settings for the Entire System	
System Name	Wireless Hotspot Gateway
Administrator Contact Information	
Suspend Warning Message	Sorry! The service is suspended. *
Internal Domain Name	gateway.example.com ☒ Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Disclaimer Page	☐ Enable ☒ Disable
Portal URL	☒ Specific ☐ Original ☐ None http://www.google.com *(e.g. http://www.example.com) Browser ID(User Agent) IEMobile/7.0.XBLWP7 (e.g. IEMobile/7.0.XBLWP7, separate by comma)
UAM Filter	Configure
User Log Access IP Address	(e.g. 192.168.2.1)
Management IP Address List	Configure
SNMP	☒ Enable ☐ Disable Configure

SNMP Configuration List			
Item	Manager IP Address	Read Community	Write Community
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Administration

The gateway supports customizable administration account types, namely **Super Group**, **Manager**, **On-Demand Manager** or **Operator**. The default predetermined group of the Administrator is Super group, and the username and password are as follows:

Admin: The administrator can access all configuration pages of the gateway.

Username: **admin**

Password: **admin**



The login page features a dark blue header with the NetCommWireless logo. On the left, there is a small inset image of two women working at a computer. To the right of the image, there are two input fields labeled 'Username:' and 'Password:'. Below the password field is a blue link that says 'Change password?'. At the bottom right, there is a yellow 'Login' button.

After a successful login to the gateway, the web management interface appears.



Admin is classified under Super Group, with all access and configuration authorities. Super Group members can generate other administrative accounts (Manager, OnDemand Manager and Operator) and configure Password Safety and Group Permission Settings.


System


Users


Network


Utilities


Status

Administrator Account

Backup & Restore

System Upgrade

Restart

Network Utilities

Certificate

[Main Menu](#) > [Utilities](#) > Administrator Account

Generate Admin Account

Name	
Password	
Confirm Password	
Group	Super Group

Apply
Cancel

Admin Account Configuration

Password Safety Settings	Configure
Group Permission Settings	Configure

Password Safety Settings:

Password rules and requirements can be configured here to facilitate additional security. The following parameters can be configured: Password Complexity, Admin Login Retry Times, Password Expire, and Admin Login Reuse Times.

Safety Setting	
Complexity Checking	☒ Enable ☐ Disable Min Password Length 2 * (2~20) Min Password Category 2 * (2~4)
Admin Login Retry Times	☒ Enable ☐ Disable Retry Times 5 *
Password Expire	☒ Enable ☐ Disable Expire Password Days 90 *
Admin Login Reuse Times	☒ Enable ☐ Disable Reuse Times 6 *

Apply
Cancel

There are three other default Administrative Account groups with predetermined permission settings, and these permission settings can be customized.

Manager: The manager can only access the configuration pages under **User Authentication** to manage the user accounts.

Authentication Settings		
Auth Option	Auth Database	Postfix
Server 1	LOCAL	local
Server 2	RADIUS	radius1
Server 3	RADIUS	radius2
On-demand User	ONDEMAND	ondemand
FREE	FREE	N/A

Operator: The operator can only access the configuration page of **Create On-demand User** to create new on-demand user accounts and print out the on-demand user account receipts.

On-demand Account Creation					
Plan	Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Cut-off	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create

OnDemand Manager: The OnDemand Manager can only access the **application programming interface** and generate on-demand user accounts from the API.

There are three additional custom groups for administrators to customize permission settings.

Select Group		
Super Group		
Super Group		
Manager		
Operator		
OnDemand Manager		
Custom 1		
Custom 2		
Custom 3		
Setting Permission		
	☒ Private ☒ Public	
System	☒ main ☒ WAN ☒ IPv6 ☒ Service Zones	☒ General ☒ WAN Traffic ☒ LAN Port Mapping
Users	☒ main ☒ Black List ☒ Policy ☒ Firewall ☒ Specific Route ☒ Additional Control	☒ Authentication ☒ Group ☒ Schedule ☒ QoS ☒ Privilege ☒ Operator

Note: To logout, simply click the Logout icon on the upper right corner of the interface to return to the login screen.

Changing Admin Passwords

To configure Admin passwords, go to: *Utilities >> Administrator Account*.

There are four predetermined levels of authority: **Super Group**, **Manager**, **Operator**, and **On-Demand Manager**. The usernames and passwords can be configured at: **Utilities >> Administrator Account**. Clicking on the hyperlink of the Name allows the administrator to change passwords.

The administrator can change the passwords here. Click Admin name on the Admin List, Enter original and new password and click **Apply** to activate the new password.

Note: Only admin has the authority to change password.

Admin Editing and Password Safety Setting	
Name	admin
Original Password	*
New Password	*
Verify Password	*

Caution: If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface via the serial console port.

Backup / Restore and Reset to the Factory Default

To configure Backup / Restore and Reset to Factory Default, go to: **Utilities >> Backup & Restore**.

This function is used to backup/restore the gateway settings. Also, the gateway can be restored to the factory default settings here.

Backup System Settings	
Backup	

Restore System Settings	
File Name	Browse...
	☒ Keep WAN setting and Management IP Address List. ☐ Keep LAN, Alias and DHCP setting. ☐ Keep Certificate. ☐ Keep Account.
Restore	

Reset to the Factory Default	
Reset	

Backup System Settings: Click **Backup** to create a .db database backup file and save it on disk.



Restore System Settings: Click **Browse** to search for a .db database backup file created by the gateway and click **Restore** to restore to the same settings at the time when the backup file was saved.

Reset to Factory Default: Click **Reset** to load the factory default settings of the gateway.

Firmware Upgrade

To configure Firmware Upgrade, go to: **Utilities >> System Upgrade**.

The administrator can download the latest firmware from the website and upgrade the system here. Select the latest firmware with **Browse** button, then click **Apply**, the system will upload the file and restart to perform the upgrade process. The firmware upgrade process can also be done via FTP. It might take a few minutes before the upgrade process completes and the new firmware's WMI interface appears.

System Firmware Upgrade	
Current Version	1.00.00
File Name	Browse... No file selected. Apply
Upgrade by FTP	IP Address: Port: Anonymous ☒ Yes ☐ No File Name Apply ex: file name or dir/file name

Note: For maintenance purposes, we strongly recommend you to backup the system settings before the upgrade.

Note: After clicking Apply, the system will begin uploading the chosen firmware into the system. Once the upload process is complete, the system will restart to activate the new firmware. The entire process may take a few minutes until the new firmware WMI appears. When restart is complete, system will not lease IP. So, please use static IP PC to upgrade system firmware.

Caution:

1. Firmware upgrade may cause the loss of some data. You may need to manually backup user account information, please refer to the release notes for the limitation before upgrading.
2. Do not power on/off the system during the upgrade or restart process. It may damage the system and cause malfunction.

Restart

To perform system restart, go to: **Utilities >> Restart**.

This function allows the administrator to safely restart the gateway, and the process takes approximately three minutes. **Reason** for restarting the system can be entered for record purposes. Click **YES** to restart the gateway; click **NO** to go back to the previous screen. Do NOT power off during system restart as this might damage the system. If the power needs to be turned off, it is highly recommended to restart the gateway first and then turn off the power after completing the restart process.

Administrator Account
Backup & Restore
System Upgrade
Restart
Network Utilities
Certificate

Main Menu > Utilities > Restart

Do you want to **RESTART the system?**

Reason:

Caution: The connection of all online users to the system will be disconnected when system is in the process of restarting.

Network Utility

To configure Network Utility, go to: **Utilities >> Network Utilities**.

System provides some network utilities for administrators. Both IPv4 and IPv6 are supported.

Wake-on-LAN is for waking up remote devices that supports Wake-on-LAN feature by entering the MAC address of the target device and then press **Wake Up** button.

Ping is to see whether a destination host is reachable and alive by entering the destination host's domain name or IP address and then press **Ping** button.

Trace Route displays the actual route taken to reach the destination host. Entering the destination host's domain name or IP address and then press **Start** button to see the route.

ARP Table is for displaying ARP information stored on the system.

Network Utilities			
Wake-on-LAN		(MAC, e.g. XX:XX:XX:XX:XX:XX)	Wake Up
IPv4	Ping	(IP/Domain Name)	Ping
	Trace Route	(IP/Domain Name)	Start Stop
	ARPing	(IP/Domain Name) Interface WAN1 ▼	ARPing
	ARP Table	Show	
IPv6	Ping6	(IP/Domain Name)	Ping6
	Trace Route 6	(IP/Domain Name)	Start Stop
	Neighbor Discovery	(IP/Domain Name) Interface WAN1 ▼	Discovery
	Neighbor Cache	Show	

Wake-on-LAN

This allows the system to remotely boot up a power-down computer connected to a LAN port with Wake-On-LAN feature enabled in its BIOS. Enter the MAC Address of the desired device and click **Wake Up** to execute this function.

Ping

It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.

Trace Route

It allows administrator to find out the real path of packets from the gateway to a destination using IP address or Host domain name.

Show ARP Table

It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).

Monitor IP Link

To configure Monitor IP Link, go to: **Network >> Monitor IP**.

The gateway will send out a packet periodically to monitor the connection status of the IP addresses on the list. On each monitored item with a WEB server running, administrators may add a link for easy access by entering the IP, selecting the **Protocol** to *http* or *https* and then clicking **Create**. After clicking **Create**, the IP address will become a hyperlink, and administrators can easily access the host remotely by clicking the hyperlink. Click the **Delete** button to remove the hyperlink if needed.

Monitor IP List				
No.	Protocol	IP Address	Hyperlink	Remark
1	http ▾		Create	
2	http ▾		Create	
3	http ▾		Create	
4	http ▾		Create	
5	http ▾		Create	
6	http ▾		Create	
7	http ▾		Create	
8	http ▾		Create	
9	http ▾		Create	
10	http ▾		Create	

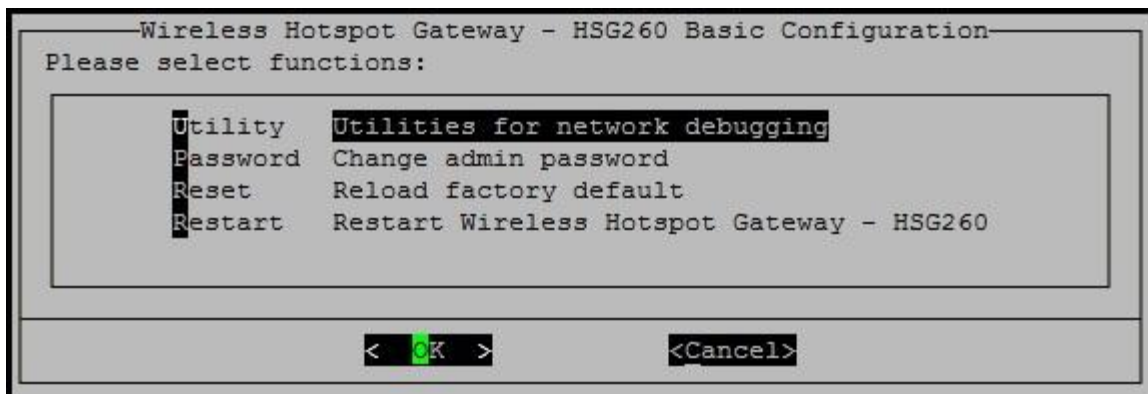
Console Interface

Via the console port, administrators can enter the console interface to handle problems and situations occurred during operation. In order to connect to the console port of the gateway, a console, modem cable, and a terminal simulation program, such as the Hyper Terminal are needed.

If a Hyper Terminal is used, please set the parameters as **9600, 8, None, 1, None**.

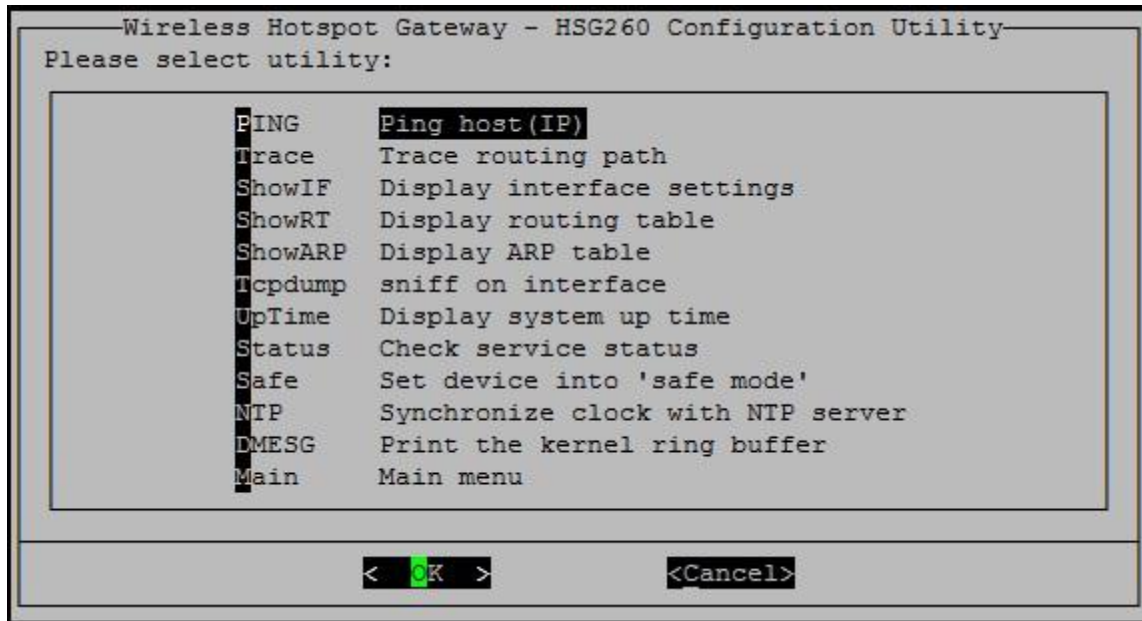
Caution: The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the Enter key to make selection or confirm what you enter.

Once the console port of the gateway is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys so that the terminal simulation program will send some messages to the system, and the welcome screen or main menu should appear. If the welcome screen or main menu of the console still does not pop up, please check the connection of the cables and the settings of the terminal simulation program.



Utilities for network debugging

The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follows:



Ping host (IP): By sending ICMP echo request to a specified host and waiting for the response to test the network status.

Trace routing path: Trace and inquire the routing path to a specific target.

Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and Netmask.

Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.

Display ARP table: The internal ARP table of the system is displayed.

Sniff on interface: This is used to confirm if data packets are passing through the interface.

Display system up time: The system life time (time for system being turned on) is displayed.

Check service status: Check and display the status of the system.

Set device into "safe mode": This is used if the administrator is unable to use Web Management Interface via browser when the system fails inexplicitly. The administrator can choose this utility and set it into safe mode, which enables him to manage this device with browser again.

Synchronize clock with NTP server: Immediately synchronizes the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, we must reset the internal clock through the NTP.

Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.

Main menu: Go back to the main menu.

Change admin password

Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface. The username and password is needed instead when connecting the system by SSH.

The username is "admin" and the default password is also "admin", which is the same as for the web management interface. Password can also be changed here. If administrators forget their password and are unable to log in to the management interface from the web or the remote end of the SSH, they can still use the null modem to connect to the console management interface and set the administrator's password again.

Caution: Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the gateway Admin username and password after your first login to the system.

Reload factory default

Choosing this option will reset the system configuration to factory defaults.

Restart the HSG

Choosing this option will restart the gateway.

System Status and Reports

Viewing the Status

This section includes **System**, **Interface**, **Routing Table**, **Current Users**, **Session List**, **User Logs**, **Logs**, **DHCP Lease** and **Report & Notification** to provide system status information and online user status.

System Status

To view System Status, go to: **Status >> System**.

This section provides an overview of the system for the administrator.

System Setting Overview		
Up Time		32 min
Firmware Version		1.00.00
Build		1.9-1.5489.2.222
System Name		NetComm Wireless 11n Hotspot HS1200N
Portal URL		http://www.netcommwireless.com
SYSLOG server 1		N/A:N/A
SYSLOG server 2		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
SNMP		Disabled
User Logs	Retained Days	3 days
	Receiver's E-mail Address(es)	N/A
		N/A
		N/A
		N/A
System Time	NTP Server	N/A
	Time	2013/08/20 16:46:29 +1000
User Session Control	Idle Time Out	10Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	172.16.1.250
	Alternate DNS Server	172.16.1.251

The description of the above-mentioned table is as follows:

<u>Item</u>		<u>Description</u>
Up Time		The total time system has operated
Firmware Version		The present firmware version of the gateway
Build		The present build number of the firmware
System Name		The system name. The default is Wireless Hotspot Gateway
Portal URL		The page users are directed to after initial login success
SYSLOG server- System Log		The IP address and port number of the external SYSLOG Server. N/A means that it is not configured
SYSLOG server- On-demand Users Log		The IP address and port number of the external SYSLOG Server. N/A means that it is not configured
Proxy Server		Shows status of built-in Proxy Server
Warning of Internet Disconnection		Shows whether the status for the connection at WAN is normal or abnormal (Internet Connection Detection) and all online users are allowed/disallowed to log in the network
SNMP		Shows status of option to enable or disabled system info retrieval via SNMP protocol
User Log		The maximum number of days for the system to retain the users' information
SNMP		The email address to which the user log information will be sent
System Time	NTP Server	The network time server that the system is set to align
	Time	The system time is shown as the local time
User Session Control	Idle Time Out	The minutes allowed for the users to be inactive before their account expires automatically
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple login from the same local account
DNS	Preferred DNS Server	IP address of the preferred DNS Server
	Alternate DNS Server	IP address of the alternate DNS Server

Interface Status

To view Interface Status, go to: **Status >> Interface**.

This section provides an overview of the interface for the administrator including **WAN**, **Zone - Private** and **Zone - Public**.

Network Interface	
Select Interface	Private ▼
Service Zone - Private	Mode
	NAT
	MAC Address
	00:60:64:B3:0E:42
	IP Address
Service Zone - DHCP Server 1	Subnet Mask
	255.255.255.0
	IPv6 Address
	N/A
	Status
RF-Card 1 VAP 1	Enabled
	WINS IP Address
	N/A
	Start IP Address
	192.168.110.2
Traffic summary	End IP Address
	192.168.110.100
	Lease Time
	1440Min(s)
	BSSID
Traffic of the day	00:60:64:B3:0E:43
	ESSID
	NetComm_HS1200N_2
	Security Type
	WPA-PSK
Traffic of the Month	Associated Clients
	0
	today
	rx 425 KiB
	tx 2.11 MiB
Traffic of the top 10	= 2.52 MiB
	0.34 kbit/s
	08/15/13
	rx 1.09 MiB
	tx 3.12 MiB
	= 4.21 MiB
	0.40 kbit/s
	all time
	rx 8.79 MiB
	tx 95.52 MiB
	= 104.31 MiB
	since 01/05/00
	Aug '13
	rx 3.07 MiB
	tx 16.14 MiB
	= 19.20 MiB
	0.09 kbit/s
	Apr '00
	rx 793 KiB
	tx 17.48 MiB
	= 18.25 MiB
	0.06 kbit/s
	Legend: rx tx
	Bar chart showing traffic volume over time (kbit/s vs date).
	16151 mStat / Teemu Toivola
	Table with 5 columns: day, rx, tx, total, avg. rate. Rows include dates from 01/05/00 to 08/20/13 and an estimated row.
	Legend: rx tx
	Bar chart showing daily traffic volume over time (kbit/s vs date).
	16151 mStat / Teemu Toivola
	Table with 5 columns: month, rx, tx, total, avg. rate. Rows include Jan '00, Mar '00, Apr '00, Aug '13, and an estimated row.
	Legend: rx tx
	Bar chart showing monthly traffic volume over time (kbit/s vs date).
	16151 mStat / Teemu Toivola
	Table with 6 columns: #, day, rx, tx, total, avg. rate. Rows include dates from 03/15/00 to 01/05/00.
	Legend: rx tx
	Bar chart showing top 10 traffic volume over time (kbit/s vs date).
	16151 mStat / Teemu Toivola

<

The description of the above-mentioned table is as follows:

<u>Item</u>		<u>Description</u>
WAN	Mode	Shows WAN interface settings: Static, Dynamic, PPPoE or PPTP
	MAC Address	The MAC address of the WAN port
	IP Address	The IP address of the WAN port
	Subnet Mask	The Subnet Mask of the WAN port
	IPv6 Address	The IPv6 address of WAN port if applicable
	IPv6 Prefix	The IPv6 prefix if applicable
Zone - General	Mode	The operation mode of the zone
	MAC Address	The MAC address of the zone
	IP Address	The IP address of the zone
	Subnet Mask	The Subnet Mask of the zone
	IPv6 Address	The IPv6 address of the zone if applicable
Zone - DHCP	Status	Enable/disable stands for the status of the DHCP server in this zone
	WINS IP Address	The WINS server IP on DHCP server. N/A means that it is not configured
	Start IP Address	The start IP address of the DHCP IP range
	End IP address	The end IP address of the DHCP IP range
	Lease Time	Minutes of lease time of the IP address
Zone - VAP	BSSID	The BSSID of this zone
	ESSID	The ESSID of this zone
	Security Type	The current security type of this zone
	Associated Clients	The number of associated clients in this zone

Routing Table

To view System Status, go to: **Status >> Routing Table**.

All the **Policy** Routing rules and **Global Policy** Routing rules for both IPv4 and IPv6 will be listed here. It will also show the **System** Routing rules specified by each interface. The following depicts an image for the IPv4 Routing Table.

Policy 1			
Destination	Subnet Mask	Gateway	Interface
Policy 2			
Destination	Subnet Mask	Gateway	Interface
Policy 3			
Destination	Subnet Mask	Gateway	Interface
Policy 4			
Destination	Subnet Mask	Gateway	Interface
Policy 5			
Destination	Subnet Mask	Gateway	Interface
Interface			
Destination	Subnet Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	Private
192.168.11.0	255.255.255.0	0.0.0.0	Public
169.254.0.0	255.255.0.0	0.0.0.0	Private
10.29.0.0	255.255.0.0	0.0.0.0	WAN
System			
Destination	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	10.29.0.1	WAN

Policy 1~5: Shows the information of the individual Policy from 1 to 5.

Global Policy: Shows the information on the Global Policy.

System: Shows the information on the system administration.

Destination: The Destination IP address.

Subnet Mask: The Subnet Mask of the IP address range.

Gateway: The Gateway IP address of the interface.

Interface: Including **WAN**, **Private** and **Public**.

Current Users

To view Current Users, go to: **Status >> Current Users**.

On this page, each online user's information including Username, IP Address, MAC Address, IPv6 Address, Pkts In, Bytes In, Pkts Out, Bytes Out, Service Zone/VLAN, Group/Policy, Authentication Method/Authentication Database, Online/Idle and Kick Out will be shown. Administrators can force out a specific online user by clicking the hyperlink of **Kick Out**. Click **Refresh** to update the current users list.

Online Users List							
No.	Username	MAC Address	Pkts In/Out	SZ / VLAN	Auth. Method	Online (Sec.)	Kick Out
	IP Address	IPv6 Address	Bytes In/Out	Group / Policy	Auth. Database	Idle (Sec.)	

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

[Refresh](#)

Non-Login Devices shows users that have acquired an IP address from the system's DHCP server but have not yet been authenticated, either under the LAN or remotely tunneled site. This feature is designed for administrators to keep track of systems' resources from being exhausted. The list shows the client's **MAC Address**, **IP Address** and associated **VLAN ID**, as well as the **Service Zone**.

Non-Login Device List			
MAC Address	IP Address	VLAN ID	Service Zone

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

[Refresh](#)

The **On-demand Roaming Out User List** shows the users that are authenticated by other gateways using this gateway's On-demand database as RADIUS database.

On-demand Roaming Out User List						
Name	IP Address	MAC Address	NAS ID	Session Time	Bytes In / Out	Login Time
					Pkts In / Out	Last Update Time

(Total:0) [First](#) [Previous](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

[Refresh](#)

[Refresh](#)

Session List

This page allows the administrator to inspect sessions currently established between a client and the system. Each result displays the IP and Port values of the Source and Destination. You may define the filter conditions and display only the results you desire.

System
Users
Access Points
Network
Utilities
Status

System
Interface
HW
Routing Table
Current Users
Session List
User Logs
Logs
DHCP Lease
Report & Notification

[Main Menu](#) > [Status](#) > Session List

Filter					
Address Family	Protocol	Source IP	Port	Destination IP	Port
IPv4	All				

[Apply Filter](#)

Display Mode: ALL

(Total:133) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page 1 (Page:1/7) Row per Page: 20

Session List							
No	Protocol	Source IP	Port	Destination IP	Port	State	Timeout
1	udp	192.168.1.254	36031	168.95.1.1	53	UNREPLIED	1
2	udp	192.168.1.254	49431	168.95.1.1	53	UNREPLIED	0

User Log

To view User Log, go to: **Status >> User Log**.

This page is used to check the traffic history of the gateway. The history of each day will be saved separately in the RAM memory for at least 3 days (72 full hours). The system also keeps a cumulated record of the traffic data generated by each user in the last 2 calendar months.

Users Log		
Date	Size (Byte)	
2012-07-10	131	
2012-07-09	131	
2012-07-08	131	
On-demand Users Log		
Date	Size (Byte)	
2012-07-10	186	
2012-07-09	186	
2012-07-08	186	
Roaming Out User Log		
Date	Size (Byte)	
2012-07-10	106	
2012-07-09	106	
2012-07-08	106	
Roaming In User Log		
Date	Size (Byte)	
2012-07-10	173	
2012-07-09	173	
2012-07-08	173	
Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2012-07	0	Download
2012-06	0	Download

Caution: Since the history is saved in the RAM memory, if you need to restart the system at the same time, please keep the history, manually by copying and saving the traffic history information before restarting.

If the Receiver **E-mail Address(es)** has been entered under the **Notification Settings** page, the system will automatically send out these history information to that specified email address.

Users Log

All user activities on the system within 72 hours excluding other user logs such as On-demand user log are recorded; in date and time order. Each line is a traffic history record consisting of 17 fields, including **Date, Type, Name, IP, IPv6, MAC, Pkts In, Bytes In, Pkts Out, Bytes Out**, and other information of the user activities.

On-demand User Log

Each line is a on-demand user log record consisting of 25 fields, **Date, System Name, Type, Name, IP, MAC, Pkts In, Bytes In, Pkts Out, Bytes Out, Activation Time, 1st Login Expiration Time, Remark**, and other information, of On-demand user activities are included.

Roaming Out User Log

Each line is a roaming out traffic history record consisting of 14 fields, **Date, Type, Name, NSID, NASIP, NASPort, UserMAC, SessionID, SessionTime, Bytes in, Bytes Out, Pkts In, Pkts Out** and **Message**, of user activities.

Roaming In User Log

Each line is a roaming in traffic history record consisting of 22 fields, **Date, Type, Name, NSID, NASIP, NASPort, UserMAC, UserIP, SessionID, SessionTime, Bytes in, Bytes Out, Pkts In, Pkts Out, Message**, and other information of user activities are included.

Local User Monthly Network Usage Report

To view Local User Monthly Network Usage, go to: **Status >> User Log**.

Monthly Network Usage of Local User

The system keeps a cumulated record of the traffic data generated by each Local user in the last 2 calendar months. Each line in the 'Monthly Network Usage of Local User' record(hyperlinked) consists of 6 fields, **Username**, **Connection Time Usage**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out** of user activities.

Username: Username of the local user account.

Connection Time Usage: The total time used by the user.

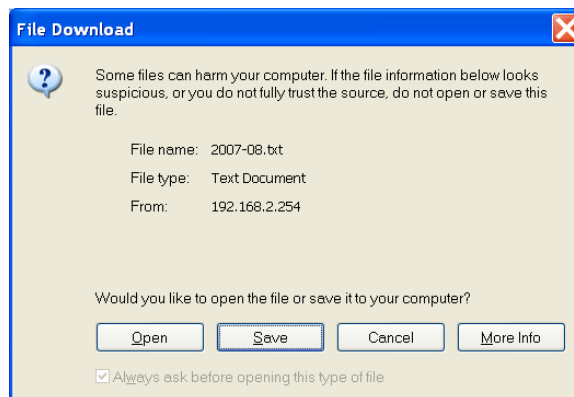
Pkts In/ Pkts Out: The total number of packets received and sent by the user.

Bytes In/ Bytes Out: The total number of bytes received and sent by the user.

Download Monthly Network Usage of Local User: Click the **Download** button for outputting the report manually to a local database.

Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2009-04	1	Download

A warning message will then appear. Click **Save** to download the record into .txt format.



System Related Logs

To configure System related logs, go to: Status >> Logs.

This page displays the system's local log information since system boot up. Administrators can examine the log entries of various events. However, since all these information are stored on volatile memory, they will be lost during a restart/reboot operation. Therefore if the log information needs to be documented, the administrator will need to make back up manually.

Logs	
System Log	Show
Web Log	Show
UAMD Log	Show
RADIUS Server Log	Show
On-demand User Billing Report Log	Show
Configuration Change Log	Show

System Log

This page displays system related logs for event tracing.

Web Log

This page shows which of the web pages have been accessed on the gateway's built-in web server.

UAMD Log

This page displays the UAM related information output from the UAM daemon.

RADIUS Server Log

This page displays the RADIUS messages that pass through the gateway.

On-demand Billing Report Log

This page displays a summary of On-demand account transactions.

Configuration Change Log

This page shows the account and IP of the user that has made configuration changes to the gateway.

DHCP Lease

To configure DHCP Lease related logs, go to: **Status >> DHCP Lease**.

The DHCP IP lease statistics can be viewed after clicking on **Show** Statistics List in this page.

Statistics of offered list

Valid lease counts of the **Last 10 Minutes**, **Hours** and **Days** are shown here. The header 1 ~ 10 are the unit multipliers. For instance the number under column 2 indicates the lease count in the last 20 minutes/hours/days, the number under column 3 indicated the lease count in the last 30 minutes/hours/days and so on.

Statistics of expired list

IP leased to clients that have expired in the **Last 10 Minutes**, **Hours** and **Days** are shown here. The header 1 ~ 10 are the unit multipliers. For instance the number under column 2 indicates the expired count in the last 20 minutes/hours/days, the number under column 3 indicates the expired count in the last 30 minutes/hours/days and so on.

Statistics of offered list										
	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	1	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	2	22	3	1	0	0	1	2	2
Last 10 Days	51	0	0	0	0	0	0	0	0	0

Statistics of expired list										
	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	0	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	0	1	0	0	0	0	0	2	1
Last 10 Days	10	0	0	0	0	0	0	0	0	0

[Refresh](#)
[Refresh](#) [Disable](#)

DHCP Lease List

Valid IP addresses issued from the DHCP Server and related information of the client using this IP address is displayed here.

DHCP Logs	
Statistics List	Show
DHCP Lease Log	Show

DHCP Lease List					
No.	IP Address	MAC Address	Host Name	Vlan	Lease Expires
1	192.168.1.4	00:40:96:a1:af:dd	x30-ac42	0	2011/03/19 17:13:49
2	192.168.1.41	00:1d:73:3b:73:3e	AC109-NB	0	2011/03/19 18:32:35
3	192.168.1.76	cc:08:e0:04:80:cf	*	0	2011/03/19 19:01:04

Notification

To configure Notification, go to: **Status >> Report & Notification**.

The gateway can automatically send the notifications of **Monitor IP Report**, **Users Log**, **On-demand User Log**, **Roaming Out Users Log**, **Roaming In Users Log**, **Firewall Log**, **Session Log** and **On-demand User Billing Report** to up to 5 particular e-mail addresses. A trial email is provided by the system for validation.

Secondly, the system supports recording of **Users Log**, **On-demand Users Log**, **Roaming Out Users Log**, **Roaming In Users Log**, **Session Log**, **Firewall Log**, and **Local HTTP Web Log**, **HTTP Web Log** and **DHCP Server Log** via external SYSLOG servers.

Thirdly, **Users Log**, **On-demand Users Log**, **Roaming Out Users Log**, **Roaming In Users Log**, **Session Log**, **On-demand User Billing Report**, **Local HTTP Web Log**, **HTTP Web Log**, **WMI Configuration Log**, **DHCP Lease Log** and **Traffic Report** can also be configured to be sent to an external FTP server. In addition, the **Event Log** section on WMI displays clients associate and disassociate messages.

E-Mail

SMTP Settings	
Receiver E-mail Address 1	
Receiver E-mail Address 2	
Receiver E-mail Address 3	
Receiver E-mail Address 4	
Receiver E-mail Address 5	
Sender E-mail Address	*
SMTP Server	*
SMTP Port	25 *
SMTP over SSL	☐ Enable ☒ Disable
SMTP Authentication	None ▼

SMTP Settings:

Receiver Email Address (es): Up to 5 e-mail addresses can be set up to receive the notification. There are eight kinds of notification for selection -- Monitor IP Report, Users Log, On-demand Users Log, Roaming Out Users Log, Roaming In Users Log, Session Log, Firewall Log, and On-demand Billing Report, check the selection box to choose the type of notification to be sent.

Sender Email Address: The e-mail address of the administrator in charge of monitoring. This will show up as the sender's e-mail.

SMTP Server: The IP address of the sender's SMTP server.

SMTP over SSL: Enable or Disable SMTP over SSL for additional security

SMTP Authentication: The system provides four authentication methods, Plain, Login, CRAM-MD5 and NTLMv1, or "None" to use none of the above. Depending on which authentication method is selected, enter the Account Name, Password and Domain.

NTLMv1 is not currently available for general use.

Plain and CRAM-MD5 are standardized authentication mechanisms while Login and NTLMv1 are Microsoft proprietary mechanisms. Only Plain and Login can use the UNIX login password. Netscape uses Plain. Outlook and Outlook express use Login as default, although they can be set to use NTLMv1.

Pegasus uses CRAM-MD5 or Login however the method to be used can not be configured.

Notification E-mail Settings:

Receiver Email Address (es): Up to 5 e-mail addresses can be set up to receive the notification. There are eight kinds of notification for selection -- Monitor IP Report, Users Log, On-demand Users Log and Session Log, check the selection box to choose the type of notification to be sent.

Interval: The time interval to send the e-mail report.

SYSLOG

SYSLOG Server Settings: There are 9 types of SYSLOG supported: **Users Log, On-demand Users Log, Roaming Out Users Log, Roaming In Users Log, Session Log, Firewall Log, Local HTTP Web Log, HTTP Web Log** and **DHCP Server Log**. Enter the IP address and Port number to specify the SYSLOG server where the report should be sent to.

Except for System Log, each supported log may be assigned *Tag* information as well as SYSLOG standard attributes *Severity* to meet the filtering requirements on the SYSLOG Server. HTTP Web Log can further select which Service Zone Web interface information to log. For each type of log information, whenever an incident occurs and data is updated, the updated log will be immediately sent to the configured SYSLOG server.

SYSLOG Settings			
SYSLOG	☒ Enabled ☐ Disabled		
SYSLOG Destinations	SYSLOG Server 1	IP Address:	Port:
	SYSLOG Server 2	IP Address:	Port:
SYSLOG Level	emergency ▼		

Note: When the number of a user's session (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this SYSLOG server.

FTP

This configuration page allows the setting of FTP Server to send, including the types of Roaming Out Users Log, Roaming In Users Log, On-demand User Billing Report, Session Log, Local HTTP Web Log, HTTP Web Log, WMI Configuration Log, DHCP Lease Log, Traffic Report, User Log or On-demand User Log based on Server Folder and Interval.

FTP Settings	
FTP Destination	IP Address: Port:
	Anonymous ☒ Yes ☐ No
	FTP Setting Test Send Test Log

FTP Server Settings

FTP Destination: Configures the common settings of the FTP server that the logs will be sent to. Further settings can be configured under Notification Settings, which includes the following:

IP Address/Port: IP address and port number of FTP server.

Anonymous: Check option "Yes" if the FTP server does not need ID credentials, otherwise check option "No" and fill in the necessary *Username* and *Password*.

FTP Setting Test: To test if the FTP settings are correct or not.

User Log: Records the User Log of the system to a specific FTP server.

On-demand User Log: Records the On-demand User Log of the system to a specific FTP server.

Roaming Out / In Users Log: Records the Roaming Out / In Users Log to a specific FTP server.

Session Log: Log each connection created by users and track the source IP/Port and destination IP/Port. Session Log will be sent to the FTP server automatically in every defined interval in Session Log email notification. Session Log allows uploading the log file to a FTP server periodically. The maximum log file size is 256K. The log file will also be sent to the FTP server once the file size reaches its maximum size.

On-demand User Billing Report: Records the On-demand User Billing Report to a specific FTP server.

Local HTTP Web Log / HTTP Web Log: Records the URL of websites visited by users accessing the internet via the gateway to a specific FTP server.

WMI Configuration Log: Records the WMI Configuration Log of the system to a specific FTP server.

DHCP Lease Log: Records the DHCP Lease Log of the system to a specific FTP server.

Traffic Report: Records the Traffic Report of the system to a specific FTP server.

Notification Settings									
	Receiver E-mail Address(es)						SYSLOG	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	☐	☐	☐	☐	☐	Detail / Send	N/A	N/A	1 Hour ▼
Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour ▼
On-demand Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour ▼
Roaming Out Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour ▼
Roaming In Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour ▼
Session Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour ▼
Firewall Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	N/A	1 Hour ▼
On-demand User Billing Report	☐	☐	☐	☐	☐	Detail / Send	N/A	☐ Detail	☐ Daily Settle Time 0 ▼ ☐ Weekly Settle Time Sun ▼ ☐ Monthly Settle Time 1 ▼
Local HTTP Web Log	N/A						☐ Detail	☐ Detail	1 Hour ▼
HTTP Web Log	N/A						☐ Detail	☐ Detail	1 Hour ▼
WMI Configuration Log	N/A						N/A	☐ Detail	1 Hour ▼
DHCP Server Log	N/A						☐ Detail	N/A	N/A
DHCP Lease Log	N/A						N/A	☐ Detail	1 Hour ▼
Traffic Report (Text) ☐ Service Zone	N/A						N/A	☐ Detail	1 Hour ▼

Server Folder: The folder in the configured FTP Server in which the sent Log will be placed.

Interval: The time interval at which the Log will be sent.

Logged Interface: The check box of Public or Private shall be checked to enable logging the HTTP Web Log of this interface.

Advanced Applications

Upload/Download Local User Accounts

To Upload / Download Local Users Accounts, go to: **Users >> Authentication**, click **Configure** for the **Local** Authentication Database. Or click **Quick Links >> Local User Management** from system Home page.

Local User Database Settings	
	Local User List
Account Roaming Out	☐ Enable ☒ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	☐ Enable ☒ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

Upload User: Click **Upload User** to enter the **Upload User from File** interface. Click the **Browse** button to select the text file for uploading user accounts, then click **Upload** to complete the upload process.

Authentication
 Black List
 Group
 Policy
 Schedule
 Firewall
 QoS
 Specific Route
 Privilege
 Additional Control
 Operator

Main Menu > Users > Authentication > Option > Local > Local User List

[Add User](#)
[Upload User](#)
[Download User](#)

[Search](#)

Local User List					
Username	Password	Applied Group	MAC Address		Del All
		Account Status	Begin Date	End Date	
Remark					
user1	user1	Group 1			Delete
		Valid			

(Total:1/3000) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

Note 1: The format of each line is "Username, Password, MAC Address, Applied Policy, Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.

Note 2: Only "0~9", "A~Z", "a~z", ".", "-", and "_" are acceptable for password field.

Upload User from File	
File Name	Browse...
Upload	

When the system uploads a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the format in the uploading file or delete the duplicated user accounts in the database then try again.

Download User: Use this function to create a .txt file with all *Local* user account information and save it on a disk.

Authentication
Black List
Group
Policy
Schedule
Firewall
QoS
Specific Route
Privilege
Additional Control
Operator

[Main Menu](#) > [Users](#) > [Authentication](#) > [Option](#) > [Local](#) > [Local User List](#) > Download

Download User to File				
Username	Password	Applied Group	MAC Address	
		Expire Time Enabled	Begin Date	End Date
		Remark		
user1	user1	1		
		Disable		

[Download](#)

RADIUS Advanced Settings

To configure RADIUS Advanced Settings, go to: **Users >> Authentication**. Click **Configure** for the **RADIUS** Authentication Database.

Complete vs. Only ID vs. Leave Unmodified

For RADIUS authentication, there is an option to send the complete username with postfix or username only.

Username Format: When the **Complete** option is checked, both the username and postfix will be transferred to the RADIUS server for authentication. On the other hand, when the **Only ID** option is checked, only the username will be transferred to the external RADIUS server for authentication. If the **Leave Unmodified** option is selected, the system will send the username to **Default Auth Server** set in **802.1X** configuration page for authentication.

NAS Identifier

System will send this value to the external RADIUS server, if needed by the external RADIUS server.

NAS Port Type

System will send this value to the external RADIUS server, if needed by the external RADIUS server.

Class-Group Mapping

This function is to assign a *Policy* to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to its assigned Group and Policy.

RADIUS Group Mapping - Server 2				
☐ Enable ☒ Disable				
No.	Class Attribute Value	Group	Remark	
1		Group 1 ▾		
2		Group 1 ▾		
3		Group 1 ▾		
4		Group 1 ▾		
5		Group 1 ▾		

Roaming Out

To configure local user Roaming Out, go to: **Users >> Authentication**, click **configure** for **Local**.

Under certain configurations, the gateway can act as a RADIUS server for Roaming Out local users logged from another system. The Local User database will act as the RADIUS user database.

Account Roaming Out & 802.1X Authentication: When Account Roaming Out is enabled; the link of Roaming Out & 802.1X Client Device Settings will be available to define the client device authorized to roam by entering the IP address, Subnet Mask, and Secret Key.

Local User Database Settings	
Local User List	
Account Roaming Out	☒ Enable ☐ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	☐ Enable ☒ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
RADIUS Client Device Settings	

802.1X Auth Setting	
Default Auth Server	Server 1 (Postfix: local) ▼ (The Auth server is for username only with ID, e.g. user1.)

RADIUS Client Device Settings					
No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out ▼	127.0.0.0	255.0.0.0 (/8) ▼	*****	
2	Disable ▼		255.255.255.255 (/32) ▼		
3	Disable ▼		255.255.255.255 (/32) ▼		
4	Disable ▼		255.255.255.255 (/32) ▼		
5	Disable ▼		255.255.255.255 (/32) ▼		

Click the hyperlink **Roaming Out & 802.1x Client Device Settings** to enter the **Roaming Out & 802.1X Client Device Settings** interface. Choose **Roaming Out** and enter the Roaming Out client's IP address and network mask and then click **Apply** to complete the settings.

In the other system, such as another gateway, set up its RADIUS server to this gateway with the same suffix and the local user in this gateway would be able to log in successfully from another gateway by RADIUS authentication.

Customizable Pages

To configure Custom Pages, go to: **System >> Service Zones**, click **Configure** in **Public** zone.

There are several user login and logout pages that can be customized by the administrator.

You can select **Default Page**, **Template Page**, **Uploaded** or **External Page**.

Custom Pages	Disclaimer Page	Configure
	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Failed Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure
	Logout Failed Page	Configure

Disclaimer Page:

The **Disclaimer Page** is for the hotspot owner or MIS staff who wants to display "terms of use" or announcement information before the user login page. Click **Configure** to access the setup page. An unauthorized client will receive a disclaimer page once opening the web browser. If a client selects "I agree" and clicks **Next**, then he or she will proceed to the User Login Page for client to login with username and password. The Disclaimer Page can be Enabled at: **System >> General**

Template Page:

To utilize the template user pages stored locally in the system, choose **Template Page** and configure the necessary settings as follows. Click **Select** (hyperlinked) to pick up a color for each item and fill in your copyright message. You can also upload a Logo image file for your template with the **Preview and Edit the Image File** button. Click **Configure** to access the setup for the corresponding page where you can change the text displayed as you wish. After setting is finished, click **Preview** to see the result. If you are happy with the customized pages, click **Apply** to activate the changes made.

Uploaded Page:

Choose the **Uploaded Page** option if you wish to upload your own html coded page. Click **Configure** for each custom page and upload the HTML file and corresponding image files and click **Apply**.

After applying the setting, the new login page can be previewed by clicking **Preview** button.

External Page:

Choose the **External Page** option if you wish to use user pages located on a designated website. Click **Configure** for each custom page and enter the URL of its corresponding external login page and click **Apply**.

After applying the setting, the new login page can be previewed by clicking **Preview** button.

Appendix A: Policy Priority

Global Policy, Authentication Policy and User Policy

The gateway supports multiple Policies, including one Global Policy and 5 individual Policies can be assigned to different Authentication Server. Global Policy is the system's universal policy and is applied to all clients, while other individual Policies can be selected and defined to be applied to any Authentication Server. For some authentication, such as Local and RADIUS, users can be assigned to different Policies individually. One user may be applied to a different policy at the same time. Which policy is actually applied to this user?

The Policy Priority is enforced as follows:

User Policy >> Authentication Policy >> Global Policy

User policy types:

For Local and RADIUS, users can be assigned to different policies individually. For example, a Local user, user01, is assigned to Policy1 and the Local Authentication Policy2. When user01 logs in to Public Zone, user01 will be governed under Policy1. This is a common case for users that can be assigned a Policy individually.

For Local and RADIUS, if these users are not assigned under any User Policy individually, they will be governed under the same policy as others within the same authentication server. For example, if the Local Authentication is assigned to Policy3, a Local user01 when logged in to Public Zone will get Policy3. This is another common case for users that are assigned Policy by the authentication server.

If a User is not assigned a Policy individually and the authentication server is also not assigned a Policy, then the Global Policy will be applied to all users. For example, a Local user, user01, is assigned to None Policy and the Local Authentication is also assigned to None Policy on User list. Then user01 logged in to Public Zone will be applied with the Global Policy.

In conclusion, the Global Policy has the lowest policy priority; the User Policy has the highest priority.

Appendix B: WDS Management

The Public Zone of the gateway supports up to 2 WDS links. WDS (Wireless Distribution System) is a function used to connect APs (Access Points) wirelessly to extend wireless coverage. The WDS management function of the system can help administrators to setup two WDS links.

To configure WDS, go to: **System >> Service Zones**, click **Configure** in **Public** zone.

General | WAN | WAN Traffic | IPv6 | LAN Port Mapping | **Service Zones** | Layer 2 Firewall

[Main Menu](#) > [System](#) > Service Zone

Service Zone Settings						
Service Zone Name	Applied Policy	IP Address	Network Alias	DHCP Pool	LAN Port Mapping	Details
	Default Authn Option	IPv6 Address			Status	
Private	Policy 1	192.168.110.1	N/A	192.168.110.2 ~ 192.168.110.100		Configure
	Disabled	N/A			Enabled	
Public	Policy 1	192.168.120.1	N/A	192.168.120.2 ~ 192.168.120.100		Configure
	Server 1	N/A			Enabled	

WDS (Wireless Distribution System) is a function used to connect **APs** (Access Points) wirelessly. The WDS management function of the system can help administrators to setup two WDS links.

WDS1 Settings : Public	
Basic	WDS Status : ☐ Enable ☒ Disable MAC Address of Remote AP :
Security	Security Type : WEP WEP Key Length : 64 bits WEP Key Format : ASCII WEP Key : 12345

WDS2 Settings : Public	
Basic	WDS Status : ☐ Enable ☒ Disable MAC Address of Remote AP :
Security	Security Type : TKIP/AES Cipher Suite : TKIP (WPA) Pre-shared Key / Pass-phrase : 12345678

WDS Status: Select **Enable** to activate this WDS link.

MAC Address of Remote AP: Enter the MAC of the remote AP that generates a WDS link with the gateway.

Security Type:

WEP: **WEP Key Length** may be 64 bits, 128 bits or 152 bits; and **WEP Key Format** can be ASCII or HEX. Enter the applicable **WEP Key**.

WPA-PSK: Select the preferred ciphering method, *TKIP* or *AES* and enter the **PSK / Pass-phrase**.

Appendix C: RADIUS Accounting

This section will briefly introduce the basic configuration of RADIUS server to work with VSA for controlling the maximum client volume usage (upload; download or upload + download traffic).

This **VSA** will be sent from the RADIUS server to the gateway along with an **Access-Accept** packet. In other words, when the external RADIUS server accepts the request, it will reply not only an **Access-Accept** but also a maximum value in bytes each user is allowed to transfer. This value can be the maximum upload traffic, the maximum download traffic, or the sum of the download and upload traffics in bytes per user. The gateway will check this value every minute; if the user traffic reaches this value, the gateway will stop the session of this user and send a "Stop" to RADIUS server.

Description

VSA is designed to allow vendors to support their own extended Attributes which are not covered in common attributes. It **MUST** not affect the operation of the RADIUS protocol.

The Attribute Type of VSA is "26" and the "Vendor ID" should be determined before proceeding to RADIUS configuration; in this example; the Vendor ID is "21920". "Attribute Number" and "Attribute Value" can then be designed to provide additional control over RADIUS.

Attribute Name	Attribute Number	Attribute Value
HSG-Byte-Amount	10	To be defined by administrator for different user groups
HSG-MaxByteIn	11	To be defined by administrator for different user groups
HSG-MaxByteOut	12	To be defined by administrator for different user groups
HSG-Byte-Amount-4GB	20	To be defined by administrator for different user groups
HSG-MaxByteIn-4GB	21	To be defined by administrator for different user groups
HSG-MaxByteOut-4GB	22	To be defined by administrator for different user groups

If the amount of traffic is larger than 4 GB, the attributes of “XXX-4GB” will be used. For example, if the amount is 5 GB, the following settings should be set: “HSG-Byte-Amount = 1048576” and “HSG-Byte-Amount-4GB = 1”.

On the other hand, when the administrator fills in all attributes, the user will be kicked out from the system if any condition is reached. For example, if the administrator sets “HSG-Byte-Amount = 1048576”; “HSG - MaxByteIn = 1048576” and “HSG- MaxByteOut = 1048576”, the user will be kicked out of the system when the downlink, uplink, or total traffic exceeds the limit.

VSA configuration in RADIUS server (IAS Server)

This section will guide you through a VSA configuration in your external RADIUS server. Before getting started, please directly or remotely access your external RADIUS server’s desktop from other PC.

Step 1

Confirm the following key elements in the RADIUS server: users, groups, and policies.

Verify whether there are already **users** in the RADIUS Server.

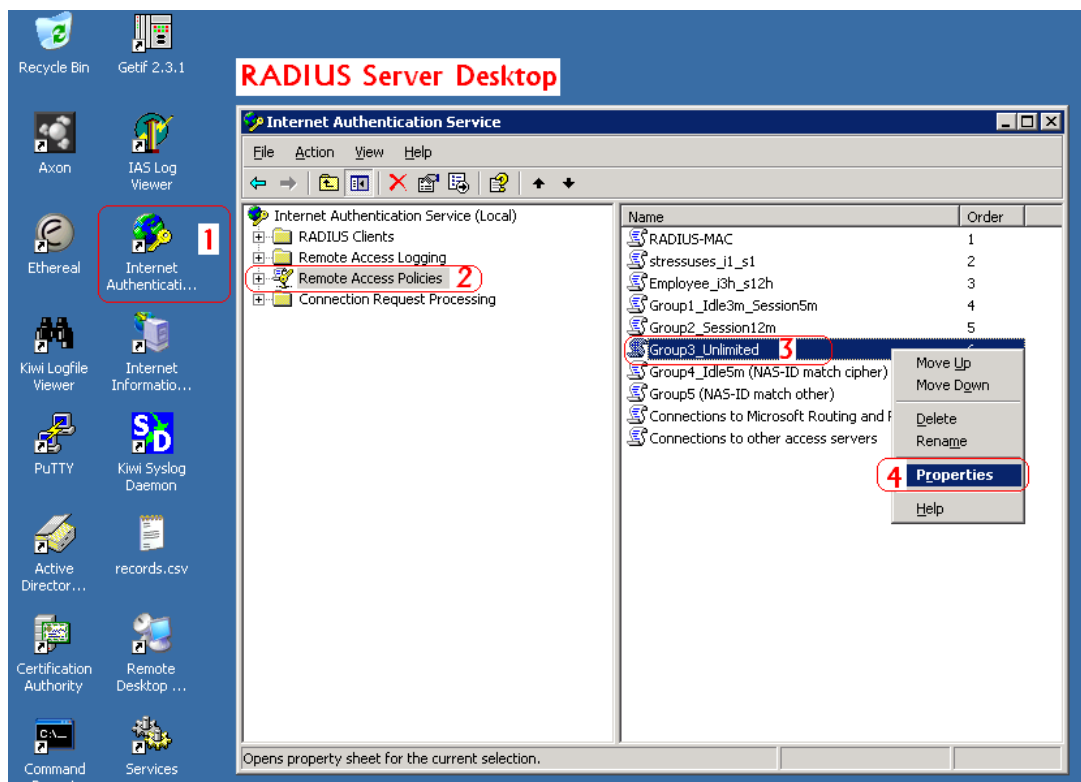
Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in the RADIUS Server.

Verify whether there are already **Policies** and assigned **Groups** belonging to these **Policies** in the RADIUS Server.

Step 2

Run “Internet Authentication Service” and open “Remote Access Policies”

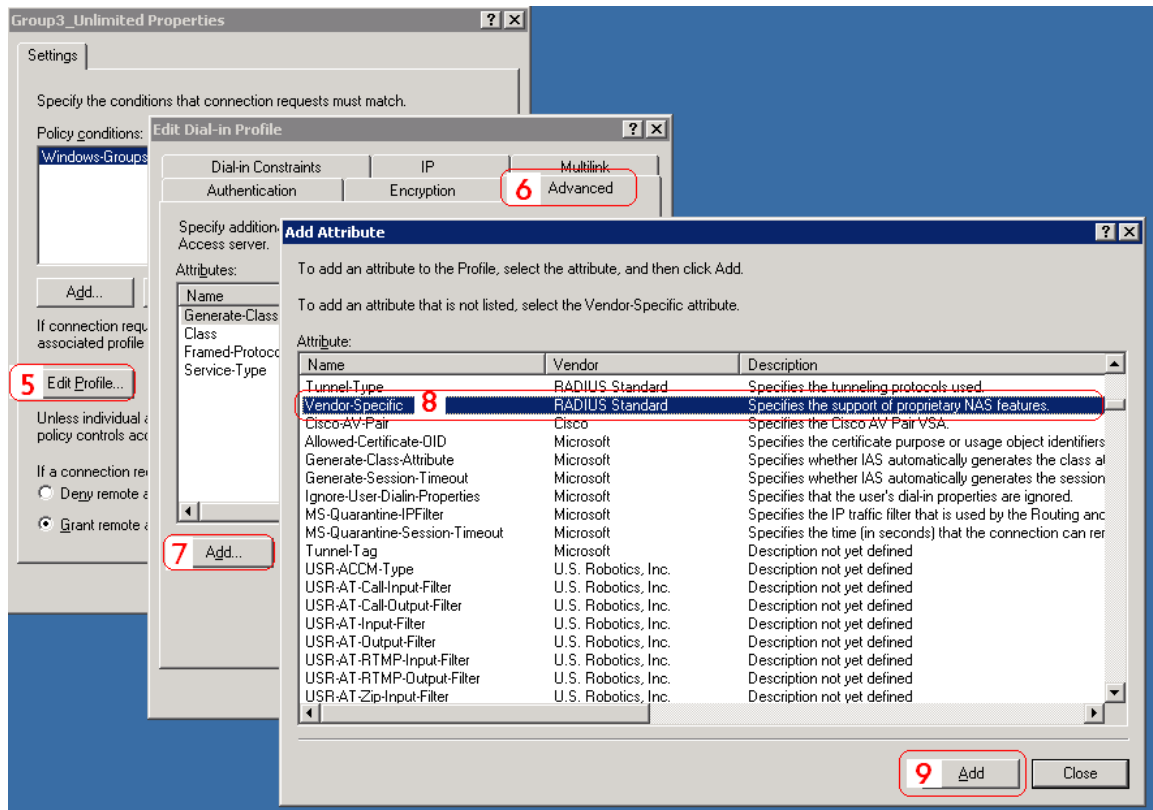
Right-click **Policy** and scroll down to the **Properties** page



Step 3

Click Edit Profile and select the Advanced Tag.

Click Add to add a new Vendor-specific attribute.



Step 4

Add a new attribute under Vendor-specific

Set "Vendor Code = 21920".

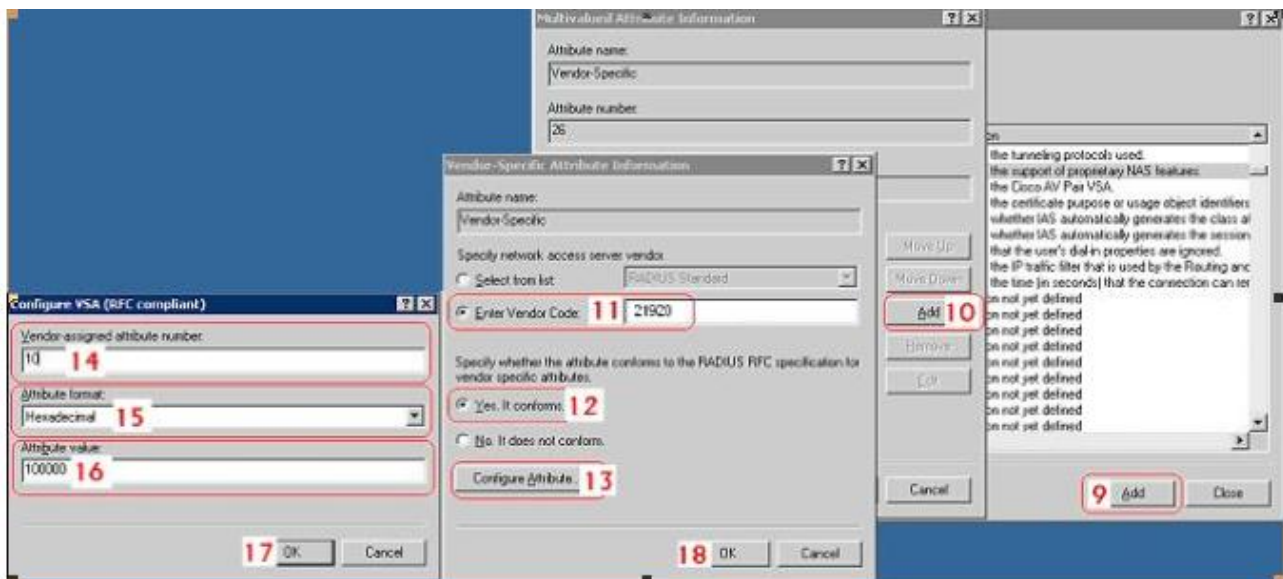
Check Yes to conform to the RADIUS RFC.

Click Configure Attribute to proceed.

Set "Vendor-assigned attribute number = 10"

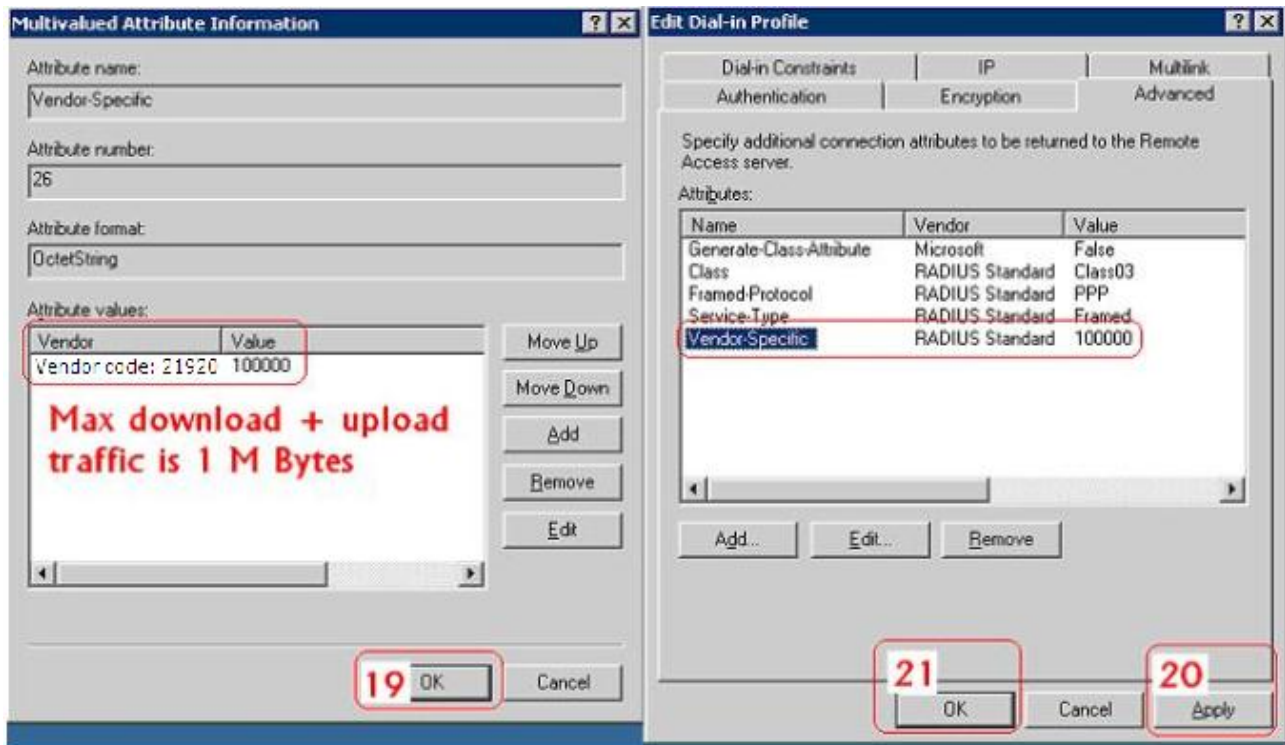
Select "Attribute format = Hexadecimal"

Set "Attribute Value = 1000000"



Step 5

Confirm whether the **Vendor-specific Attribute** has been added successfully



The image shows two side-by-side Windows XP dialog boxes. The left dialog, titled 'Multivalued Attribute Information', has fields for 'Attribute name' (Vendor-Specific), 'Attribute number' (26), and 'Attribute format' (OctetString). Below these is a table for 'Attribute values' with columns 'Vendor' and 'Value'. The first row shows 'Vendor code: 21920' and '100000'. A red box highlights the 'OK' button, which is labeled with a red '19'. The right dialog, titled 'Edit Dial-in Profile', has tabs for 'Dial-in Constraints', 'IP', 'Multilink', 'Authentication', 'Encryption', and 'Advanced'. The 'Advanced' tab is selected, showing a list of 'Attributes'. The list includes 'Generate-Class-Attribute', 'Class', 'Framed-Protocol', 'Service-Type', and 'Vendor-Specific'. The 'Vendor-Specific' attribute is highlighted with a red box. Below the list are 'Add...', 'Edit...', and 'Remove' buttons. At the bottom, there are 'OK' (labeled with a red '21'), 'Cancel', and 'Apply' (labeled with a red '20') buttons.

Vendor	Value
Vendor code: 21920	100000

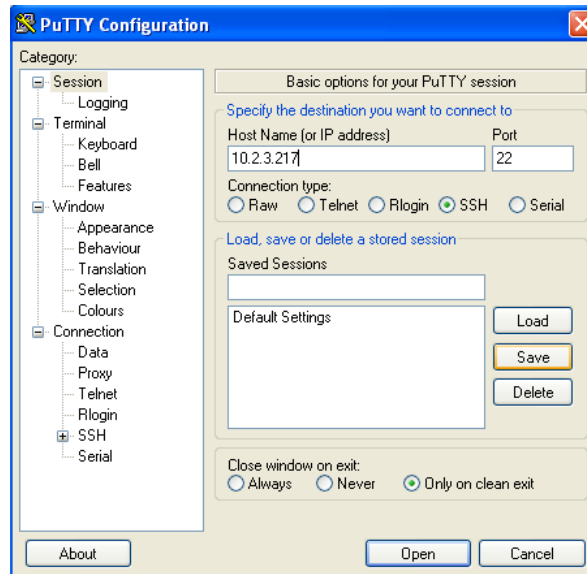
Name	Vendor	Value
Generate-Class-Attribute	Microsoft	False
Class	RADIUS Standard	Class03
Framed-Protocol	RADIUS Standard	PPP
Service-Type	RADIUS Standard	Framed
Vendor-Specific	RADIUS Standard	100000

Step 6

Follow the same steps to create other Vendor-specific Attributes if needed.

VSA configuration in RADIUS server (FreeRADIUS)

This section will guide you through **VSA** configuration with FreeRADIUS v1.0.5 running on “Fedora”. Before getting started, open the shell of RADIUS server; for example, use *Putty* to access the Linux host:



Step 1

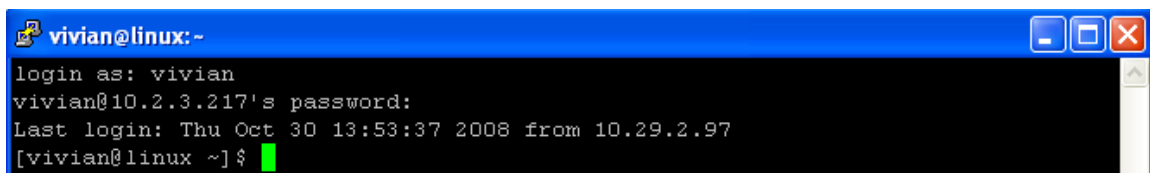
Confirm the following key elements in the RADIUS server: users, groups

Verify whether there are already **users** in the RADIUS Server.

Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in the RADIUS Server.

Step 2

Log in to the Linux host of the RADIUS server.



Step 3

Create a file “dictionary.HSG” under the “freeradius” folder.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary.
```

Step 4

Edit and save the contents of the file “dictionary.HSG” as follows:

```
VENDOR                                21920

#
#      Standard attribute
#
ATTRIBUTE      -Byte-Amount          10      interger
```

Administrator can also add other attributes as the table stated in Section 2 with the same format.

```
VENDOR                                21920
#
#      Standard attribute
#
ATTRIBUTE          -Byte-Amount          10      interger
ATTRIBUTE          -MaxByteIn             11      interger
ATTRIBUTE          -MaxByteIn             12      interger
ATTRIBUTE          -Byte-Amount-4GB       20      interger
ATTRIBUTE          -MaxByteIn-4GB         21      interger
ATTRIBUTE          -MaxByteIn-4GB         22      interger
```

Step 5

Edit the file “dictionary” under the folder “freeradius”.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary
```

Step 6

To include “dictionary.HSG” in the dictionary of RADIUS server, insert it in an incremental position as follows.

```
$INCLUDE dictionary.ascend
$INCLUDE dictionary.bay
$INCLUDE dictionary.bintec
$INCLUDE dictionary.cabletron
$INCLUDE dictionary.
$INCLUDE dictionary.cisco
#
#   This is the same as the altiga dictionary.
#
$$INCLUDE dictionary.cisco.vpn3000
$INCLUDE dictionary.cisco.vpn5000
$INCLUDE dictionary.cisco.bbsm
$INCLUDE dictionary.colubris
$INCLUDE dictionary.erx
```

Step 7

Open the “radius” database.

```
[vivian@linux ~]$ mysql -u root -p radius
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 98 to server version: 5.0.27

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Step 8

Insert **VSA** into RADIUS response. In this example, the maximum download and upload traffics in bytes for **group03 users** is 1MBytes.

```
mysql> INSERT INTO radgroupreply (GroupName,Attribute,op,Value)
VALUES ('group03', cipherium-Byte-Amount',':=', '1048576')
Query OK, 1 row affected (0.00 sec);
mysql> exit
Bye
```

Step 9

Restart RADIUS daemon to get your settings activated.

```
[vivian@linux ~] # /etc/init.d/radiusd restart
Stopping RADIUS server: [ OK ]
Starting RADIUS server: Thu Oct 30 14:26:41 2008 : Info: Starting - reading conf
figuration files ... [ OK ]
```

Appendix D: On-demand Account types & Billing Plan

This section explains the parameters as well as the different account types provided when editing billing plans in On-demand authentication.

Usage-time with Expiration Time: Users can access internet as long as account is valid with remaining quota (usable time). Users need to activate the purchased account within a given time period by logging in. It is Ideal for short-term usage, namely in coffee shops, at airport terminals, etc. This billing type only deducts quota when internet is being used. However, the count down to Expiration Time is continuous regardless of logging in or out. Account would expire when the **Valid Period** is used up or the quota depleted.

Quota is the total period of time (xx days yy hrs zz mins), during which On-demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.

Account Activation is carried out when the user logs in for the first time. Failing to do so in the period set in Account Activation will result in account expiration.

Valid Period is the valid period of usage time. After this time period, even if there is remaining quota, the account will still expire.

Price is the unit price of this plan.

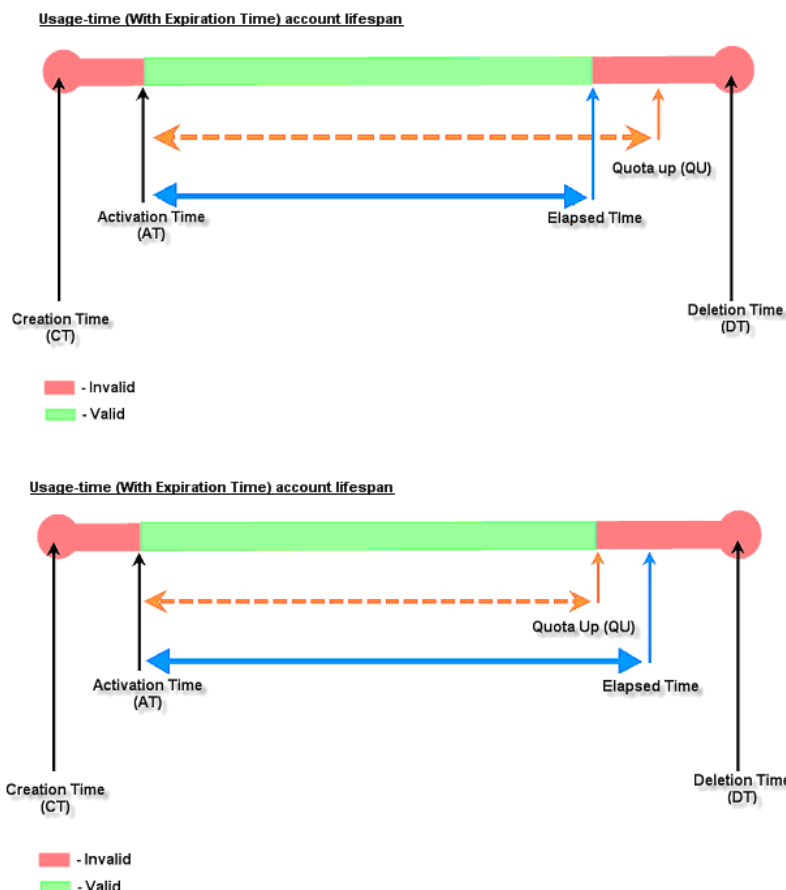
Group will be the applied Group to users created from this plan.

Reference field allows administrator to input additional information.

Editing Billing Plan	
Plan	2
Account Type	Usage-time
Expiration Time	☒ With Expiration Time ☐ No Expiration Time
Quota	1 day(s) 2 hr(s) 3 min(s) *(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Account Activation	First time login must be done within 4 day(s) 5 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 6 day(s) *(Must be larger than 0)
Price	7 (\$) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	

TIP:

If the Account Type is "Usage Time", Customer can access internet as long as the account is valid with remaining quota (connection time) and within the valid period. Customer also needs to activate the issued account within a given time period by logging in for the first time.



Usage-time with No Expiration Time: Users can access internet as long as the account has remaining quota (usable time). Users need to activate the purchased account within the given time by logging in. It is ideal for short-term usage. For example, in coffee shops, at airport terminals etc. This billing type only deducts quota while the user is using internet. Account will expire only when the quota is depleted.

Quota is the total period of time (xx days yy hrs zz mins), during which On-demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.

Account Activation is carried out when the user logs in for the first time. Failing to do so in the period set in Account Activation will result in account expiration.

Price is the unit price of this plan.

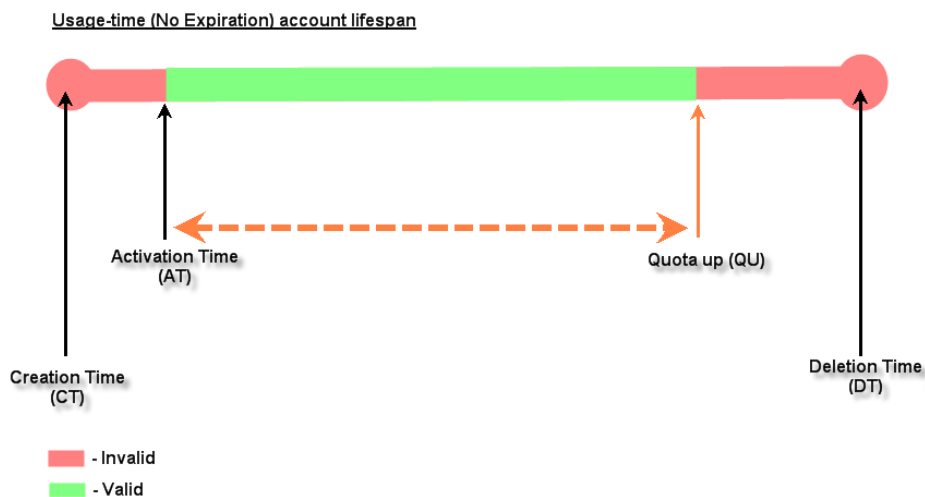
Group will be the applied Group to users created from this plan.

Reference field allows administrator to input additional information.

Editing Billing Plan	
Plan	3
Account Type	Usage-time
Expiration Time	☐ With Expiration Time ☒ No Expiration Time
Quota	day(s) hr(s) min(s) *(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Account Activation	First time login must be done within day(s) hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Price	(\$) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	

TIP:
If the Account Type is "Usage Time", Customer can access internet as long as the account is valid with remaining quota (connection time) and within the valid period. Customer also needs to activate the issued account within a given time period by logging in for the first time.

Apply Cancel



Hotel Cut-off-time: Hotel Cut-off-time is the clock time (normally check-out time) at which the on-demand account is cut off (made expired) by the system on the following day or many days later. On the account creation UI of this plan, operator can enter a Unit value which is the number of days to Cut-off-time according to customers' stay time. For example: Unit = 2 days, Cut-off Time = 13:00 then account will expire on 13:00 two days later. **Grace Period** is an additional, short period of time after the account is cut off that allows user to continue to use the on-demand account to access the Internet without paying additional fee. **Unit Price** is the daily price of this billing plan. It is mainly used in hostel (hotel?) venues to provide internet service according to guests' stay time. **Group** will be the applied Group to users created from this plan. **Reference** field allows administrator to input additional information.

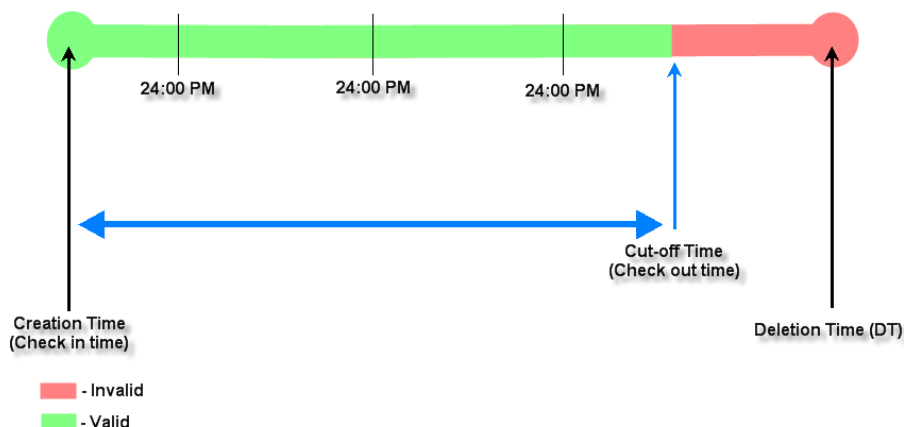
Editing Billing Plan	
Plan	5
Account Type	Hotel Cut-off-time
Hotel Cut-off Time	13 : 00 *(HH:MM; range : 00:00 ~ 23:59)
Grace Period	Account remains usable for 0 hour(s) after cut-off.
Unit Price	60 per day (\$) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	

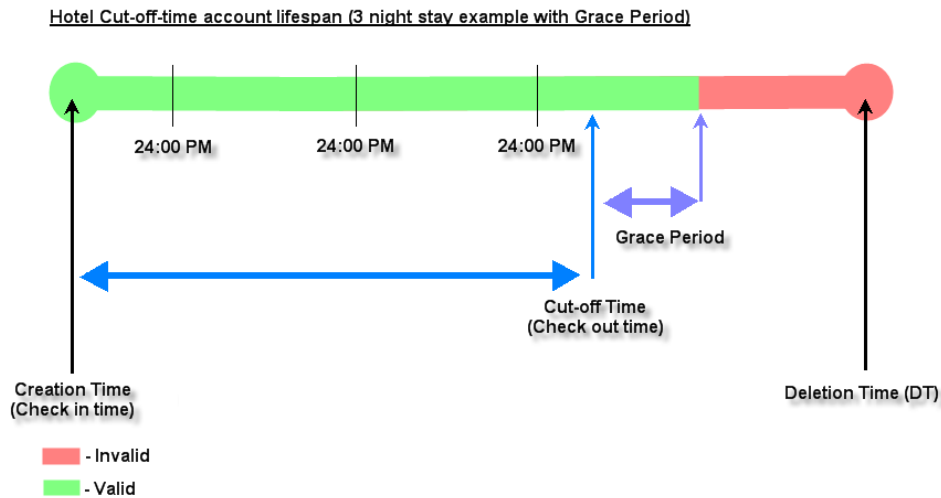
TIP:
The "Hotel Cut-off-time" Account Type is designed for hotel applications and conforms to check-in/out scenario. For cut-off applications within one day (for example, the account expires upon bookstore's closing hour ~11PM) please select "Duration Time". One-day-stay in Hotel terms is counted from a customer's check-in time to the check-out time on the following day. When a tenant checks in for one or multiple days, the operator can generate an account ticket based on the number of the over-night stay. The account will be cut-off on the specified cut-off-time (normally the hotel's check-out-time) after the number of nights specified. Since guests may hang around in the lobby for a short while after checking out, the hotel may want to specify a "Grace period" for their tenants.

Apply

Cancel

Hotel Cut-off-time account lifespan (3 night stay example)





Volume: Users can access internet as long as his/her account has remaining traffic volume quota. The account will expire when *Valid Period* has been used up or the quota is depleted. This type is ideal for small quantity of applications such as sending/receiving email, transferring a file, etc. Count down of Valid Period is continuous regardless of logging in or out.

Quota is the total Mbytes (1~2000) On-demand users are allowed to use to access the network.

Account Activation is carried out when the user logs in for the first time. Failing to do so in the period set in Account Activation will result in account expiration

Valid Period is the valid period of usage time. After this time period, the account will expire even if there is remaining quota.

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

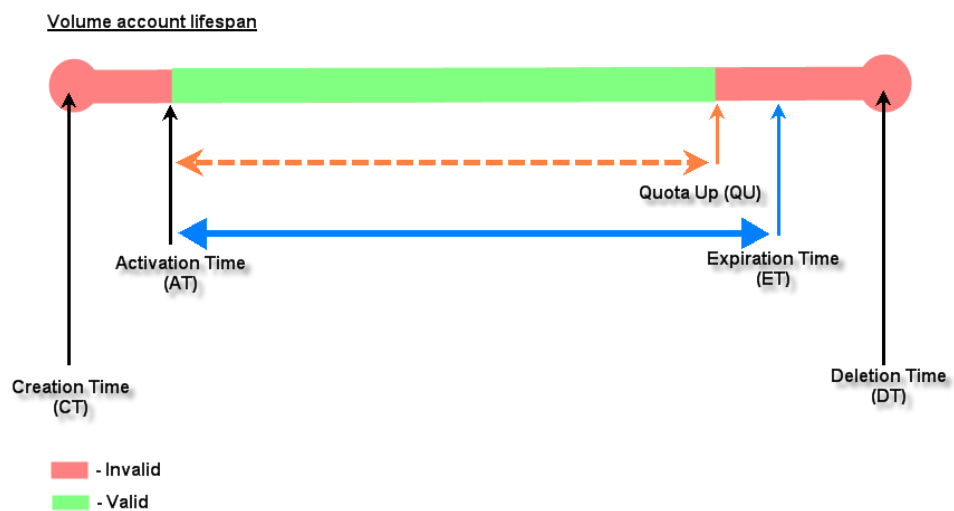
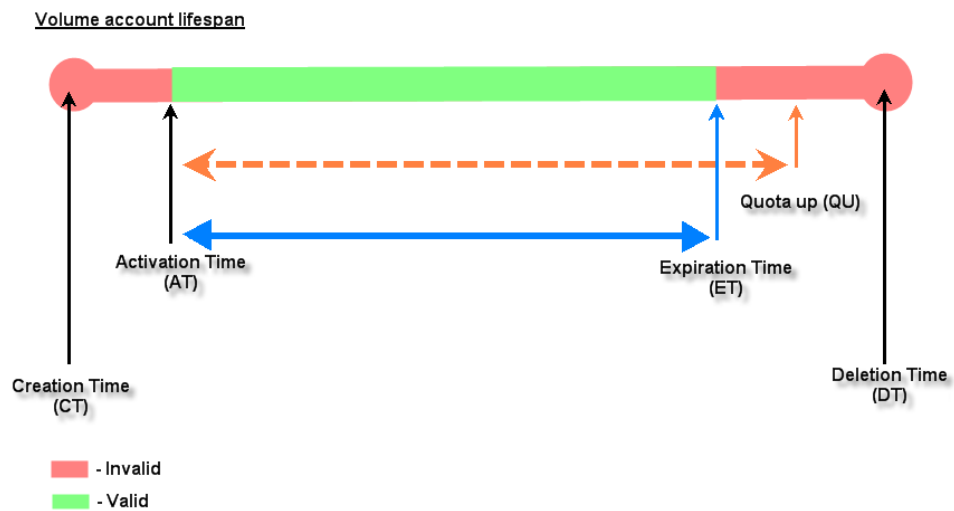
Reference field allows administrator to input additional information.

Editing Billing Plan	
Plan	1
Account Type	Volume
Quota	500 Mbyte(s) *(Range : 1 ~ 1000000)
Account Activation	First time login must be done within 1 day(s) 1 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 1 day(s) *(Must be larger than 0)
Price	1 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 4
Reference	

TIP:
If the Account Type is "Volume", Customer can access internet as long as the account is valid (within the valid period) with remaining quota (traffic volume).
Customer also needs to activate the issued account within a given time period by logging in for the first time.

Apply

Cancel



Duration-time with Elapsed Time: Account is activated upon the account creation time. Count down begins immediately after account creation and is continuous regardless of logging in or out. The account will expire once the *Elapsed Time* is reached. This billing type is ideal for providing internet service immediately after account creation throughout a specific period of time.

Begin Time is the time that the account will be activated for use. It is set to account creation time.

First time login is set to require users to log in within a specified period of time.

Elapsed Time is the time interval for which the account is valid for internet access (xx hrs yy mins).

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

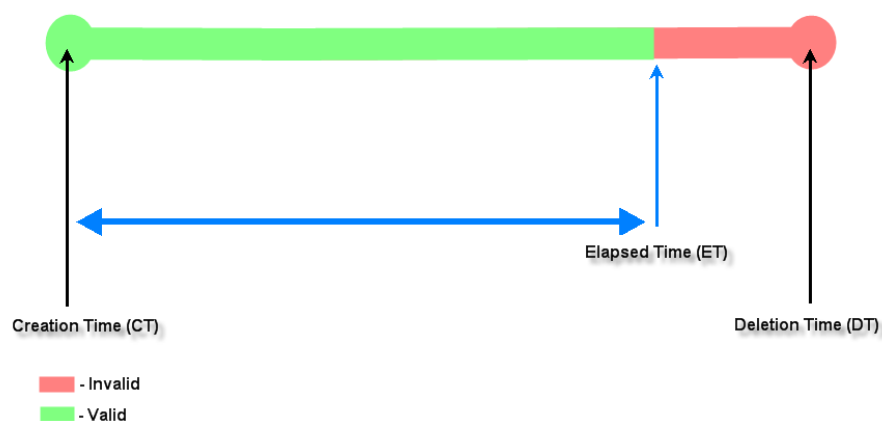
Reference field allows administrator to input additional information.

Editing Billing Plan	
Plan	1
Account Type	Duration-time ▼
Counting Method	☒ Elapsed Time ☐ Begin-and-end Time ☐ Cut-off Time
Begin Time	☒ Upon Account Creation ☐ First time login must be done within 1 day(s) 1 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Elapsed Time	1 day(s) 2 hr(s) 30 min(s) *(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Price	6 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1 ▼
Reference	

TIP:
 When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.
 1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
 2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
 3. "Begin and End Time" specifies that the account is valid between the two time points.

Apply Cancel

Duration-time (Elapsed Time) account lifespan



Duration-time with Cut-off Time: **Cut-off Time** is the clock time at which the on-demand account is cut off (made expired) by the system on that day. For example if a shopping mall closes at 23:00, operators selling on-demand tickets can use this plan to create a ticket set to be Cut-off on 23:00. If an account of this kind is created after the Cut-off Time, the account will automatically expire.

Begin Time is the time that the account will be activated for use. It is set to account creation time.

Cut-off Time is the clock time when the account will expire.

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

Reference field allows administrator to input additional information.

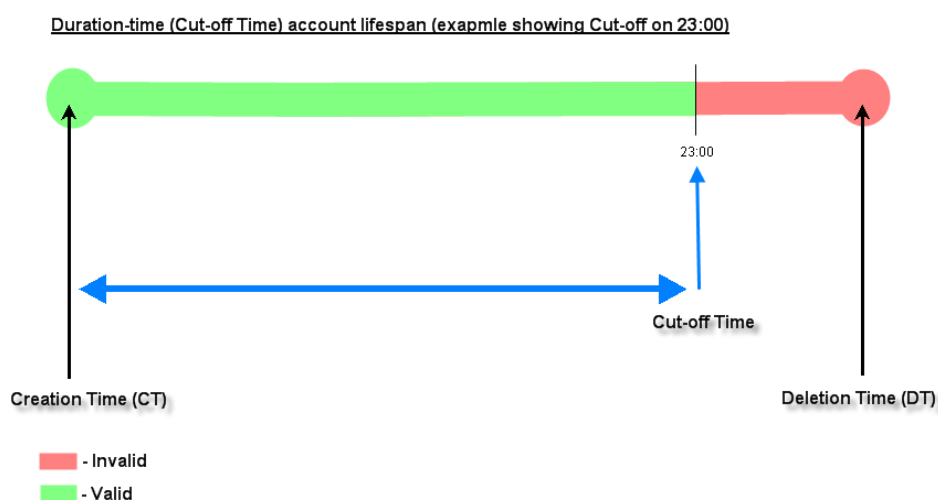
Editing Billing Plan	
Plan	1
Account Type	Duration-time
Counting Method	☐ Elapsed Time ☐ Begin-and-end Time ☒ Cut-off Time
Begin Time	Upon Account Creation
Cut-off Time	10 : 00 *(HH:MM; range : 00:00 ~ 23:59)
Price	4 (\$) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	5

TIP:
When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.

1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Date Time" specifies that the account is valid between the two time points.

Apply

Cancel



Duration-time with Begin-and End Time: This plan defines explicitly the *Begin Time* and *End Time* of the account. Count down begins immediately after account activation and expires when the *End Time* is reached. This plan is ideal for providing internet service throughout a specific period of time; for example during exhibition events or large conventions such as Computex where each registered participant will get an internet account valid from 8:00 AM Jun 1 to 5:00 PM Jun 5. Account can be created in batch similar to creating coupons.

Begin Time is the time that the account will be activated for use, defined explicitly by the operator.

End Time is the time that the account will expire, defined explicitly by the operator.

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

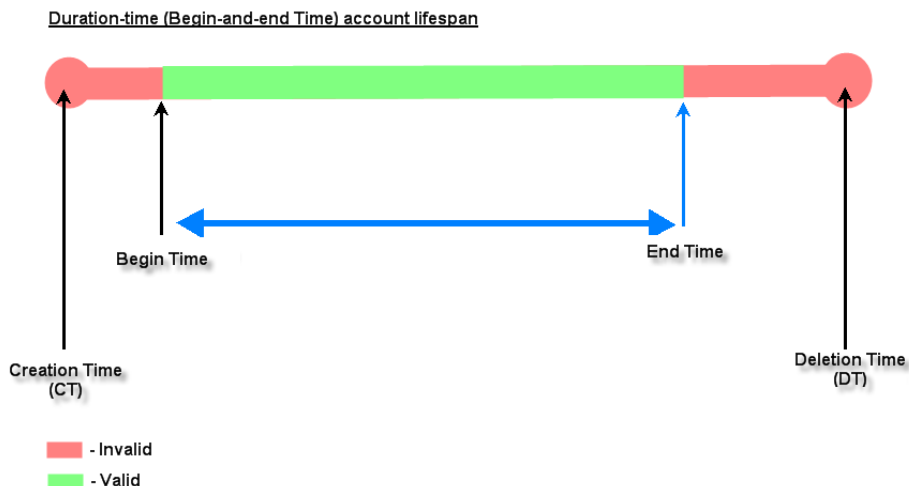
Reference field allows administrator to input additional information.

Editing Billing Plan	
Plan	6
Account Type	Duration-time
Counting Method	☐ Elapsed Time ☒ Begin-and-end Time ☐ Cut-off Time
Begin Time	00 : 01 , Jan 01 2010
End Time	03 : 03 , Jun 10 2014
Price	7000 (\$) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	

TIP:
 When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.

1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Date Time" specifies that the account is valid between the two time points.

Apply Cancel



External Payment Gateways

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via Authorize.net, PayPal, SecurePay or WorldPay, making the Hotspot an e-commerce environment for end users to pay for and obtain Internet access with credit cards.

Payments via Authorize.Net

To configure Payments via Authorize.Net, go to:

Users >> Authentication >> On-demand User >> External Payment Gateway >> Authorize.Net.

Before setting up "Authorize.Net", it is required that the merchant owners have a valid Authorize.Net account.

Authorize.Net Payment Page Configuration

External Payment Gateway	
☒ Authorize.Net	☐ PayPal
☐ SecurePay	☐ WorldPay
☐ Disable	

Authorize.Net Payment Page Configuration	
Merchant Login ID	*
Merchant Transaction Key	*
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll *
Verify SSL Certificate	☒ Enable ☐ Disable Default ▼
Test Mode	☐ Enable ☒ Disable Try Test *
MD5 Hash	☐ Enable ☒ Disable

Merchant ID: This is the "Login ID" that comes with the Authorize.Net account

Merchant Transaction Key: The merchant transaction key is similar to a password and is used by Authorize.Net to authenticate transactions.

Payment Gateway URL: This is the default website address to post all transaction data.

Verify SSL Certificate: This is to help protect the system from accessing a website other than Authorize.Net.

Test Mode: In this mode, merchants can post **test** transactions **for free** to check if the payment function works properly.

MD5 Hash: If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction or transaction response received by their server are actually sent from the Authorize.Net.

Service Disclaimer Content/ Choose Billing Plan for Authorize.Net Payment Page/Client's Purchasing Record

Service Disclaimer Content			
We may collect and store the following personal information: email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.			

Choose Billing Plan for Authorize.Net Payment Page				
Plan	Enable/Disable		Quota	Price
1	☐ Enable	☒ Disable	5 hr(s) 5 min(s)	0
2	☐ Enable	☒ Disable		
3	☒ Enable	☒ Disable	10 hr(s) 6 min(s)	9000
4	☐ Enable	☒ Disable		
5	☐ Enable	☒ Disable	Until 18:30	88
6	☐ Enable	☒ Disable		
7	☒ Enable	☒ Disable	20.73 Mbyte(s)	0.59
8	☐ Enable	☒ Disable		
9	☐ Enable	☒ Disable		
10	☒ Enable	☒ Disable	600 Mbyte(s)	6.99

Client's Purchasing Record	
Starting Invoice Number	Hotspot - 00000001 * ☐ Change the Number
Description (Item Name)	Internet Access *
E-mail Header	Enjoy Online! *

Service Disclaimer Content

View service agreements and fees for the standard payment gateway services here as well as adding a new or editing service disclaimer.

Choose Billing Plan for Authorize.Net Payment Page

These 10 plans are the plans configured in the Billing Plans page, and all previously enabled plans can be further enabled or disabled here, as needed.

Client's Purchasing Record

Starting Invoice Number: An invoice number may be provided as additional information for a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.

Description (Item Name): This is the item information to describe the product (for example, Internet Access).

Email Header: Enter the information that should appear in the header of the invoice.

Authorize.Net Payment Page Fields Configuration/ Authorize.Net Payment Page Remark Content

Authorize.Net Payment Page Fields Configuration		
Item	Displayed Text	Required
☒ Credit Card Number	Credit Card Number *	☒
☒ Credit Card Expiration Date	Credit Card Expiration Date *	☒
☒ First Name	First Name *	☒
☒ Last Name	Last Name *	☒
☒ Card Type	Card Type * ☒ Visa ☒ American Express ☒ Master Card ☒ Discover	☒
☒ Card Code	Card Code *	☒
☒ E-mail	E-mail *	☐
☐ Customer ID	Room Number *	☐
☒ Company	Company *	☐
☒ Address	Address *	☐
☒ City	City *	☐
☒ State	State *	☐
☒ Zip	Zip *	☐
☒ Country	Country *	☐
☒ Phone	Phone *	☐
☒ Fax	Fax *	☐

*Displayed text fields must be filled.

Authorize.Net Payment Page Remark Content	
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If	

Authorize.Net Payment Page Fields Configuration

Item: Check the box to show this item on the customer's payment interface.

Displayed Text: Enter what needs to be shown for this field.

Required: Check the box to indicate this item as a required field.

Credit Card Number: Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

Credit Card Expiration Date: Expiration date of the credit card. This should be entered in the format of MMYY. For example, the expiration date of July September 2009 should be entered as 0709.

Card Type: This value indicates the level of match between the Card Code entered in a transaction and the value that is on the file with a customer's credit card company. A code and narrative description are provided to indicate the results returned by the processor.

Card Code: The three- or four-digit code assigned to a customer's credit card number (at the end of the credit card number found either on the front or back of the card).

E-mail: An email address may be provided along with the billing information for a transaction. This is the customer's email address and should contain an @ symbol.

Customer ID: This is an internal identifier for customers that may be associated with the billing information for a transaction. This information field may contain any format.

First Name: The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

Last Name: The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

Company: The name of the company associated with the billing or shipping information entered on a given transaction.

Address: The address entered either in the billing or shipping information of a given transaction.

City: The city associated with either the billing address or shipping address of a transaction.

State: A state associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

Zip: The ZIP code represents a five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

Country: The country associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full name.

Phone: A phone number associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

Fax: A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

Authorize.Net Payment Page Remark Content

Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

Payments via PayPal

To configure Payments via PayPal, go to:

User >> Authentication >> On-demand User >> External Payment Gateway >> PayPal.

Before setting up "PayPal", it is required that the hotspot owners have a valid PayPal "Business Account".

After opening a PayPal Business Account, the hotspot owners should find the "**Identity Token**" of this PayPal account to continue with "PayPal Payment Page Configuration".

External Payment Gateway / PayPal Payment Page Configuration

PayPal Payment Page Configuration	
Business Account	*
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr *
Identity Token	*
Instant Payment Notification (IPN)	☒ Enable ☐ Disable ☒ Behind NAT External Gateway IP: * External Gateway Port: *
Verify SSL Certificate	☒ Enable ☐ Disable Default ▾
Currency	USD (U.S. Dollar) ▾ *

Business Account: The "Login ID" (an email address) associated with the PayPal Business Account.

Payment Gateway URL: The default website address to post all transaction data.

Identity Token: This is the key used by PayPal to validate all the transactions.

IPN behind NAT: IPN is the acronym of Instant Payment Notification which is a mechanism adopted by PayPal for identifying the outcome of a transaction. When this option is enabled, an upstream NAT server may be designated for accepting the IPN message from PayPal. This is a mandatory configuration item if the WAN IP of your gateway is not a public IP address, corresponding NAT translation configurations are necessary.

Verify SSL Certificate: This is to help protect the system from accessing a website other than PayPal

Currency: The currency to be used for payment transaction.

Service Disclaimer Content / Choose Billing Plan for PayPal Payment Page

Service Disclaimer Content
We may collect and store the following personal information: email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us. If the information you provide cannot be verified, we may

Choose Billing Plan for PayPal Payment Page			
Plan	Enable/Disable		Quota
1	☐ Enable	☒ Disable	5 hr(s) 5 min(s)
2	☐ Enable	☒ Disable	
3	☒ Enable	☒ Disable	10 hr(s) 6 min(s)
4	☐ Enable	☒ Disable	
5	☐ Enable	☒ Disable	Until 18:30
6	☐ Enable	☒ Disable	
7	☒ Enable	☒ Disable	20.73 Mbyte(s)
8	☐ Enable	☒ Disable	
9	☐ Enable	☒ Disable	
10	☒ Enable	☒ Disable	600 Mbyte(s)
			Price
			0
			9000
			88
			0.59
			6.99

Service Disclaimer Content: View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

Choose Billing Plan for PayPal Payment Page: These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

Client's Purchasing Record / PayPal Payment Page Remark Content

Client's Purchasing Record	
Starting Invoice Number	Hotspot: [0000000] * ☐ Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

PayPal Payment Page Remark Content
(A) Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button,

Client's Purchasing Record:

Starting Invoice Number: An invoice number may be provided as additional information for the transaction. This is a reference field that may contain any sort of information.

Description: Enter the product/service description (e.g. wireless access service).

Title for Message to Seller: Enter the information that will appear in the header of the PayPal payment page.

PayPal Payment Page Remark Content: The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe caution for making a payment via PayPal.

Payments via SecurePay

To configure Payments via SecurePay, go to: **Users >> Authentication >> On-demand User>> External Payment Gateway >> SecurePay.**

Before setting up "SecurePay", it is required that the hotspot owners have a valid SecurePay "Merchant Account" from its official website.

External Payment Gateway			
☐ Authorize.Net	☐ PayPal	☒ SecurePay	☐ WorldPay
☐ Disable			

SecurePay Payment Page Configuration	
Merchant ID	*
Merchant Password	*
Payment Gateway URL	https://www.securepay.com.au/xmlapi/payment *
Verify SSL Certificate	☒ Enable ☐ Disable Default ▼
Currency	AUD (Australian Dollar) ▼ *

Service Disclaimer Content
We may collect and store the following personal information: physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

Choose Billing Plan for SecurePay Payment Page			
Plan	Enable/Disable	Quota	Price
1	☐ Enable ☒ Disable		
2	☐ Enable ☒ Disable		
3	☐ Enable ☒ Disable		
4	☐ Enable ☒ Disable		
5	☐ Enable ☒ Disable		
6	☐ Enable ☒ Disable		
7	☐ Enable ☒ Disable		
8	☐ Enable ☒ Disable		
9	☐ Enable ☒ Disable		
10	☐ Enable ☒ Disable		

SecurePay Payment Page Remark Content
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.

SecurePay Page Configuration

Merchant ID: The ID that is associated with the Merchant Account.

Merchant Password: This is the key used by Secure Pay to validate all the transactions.

Payment Gateway URL: The default website address to post all transaction data.

Verify SSL Certificate: This is to help protect the system from accessing a website other than Secure Pay.

Currency: The currency to be used for the payment transactions.

Service Disclaimer Content

View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

Choose Billing Plan for SecurePay Payment Page

These 10 plans are the plans in Billing Configuration, and the desired plan(s) can be enabled.

SecurePay Payment Page Remark Content

The message content will be displayed as a special notice to end customers.

Payments via World Pay

To configure Payments via WorldPay, go to:

Users >> Authentication >> On-demand User >> External Payment Gateway >> WorldPay.

WorldPayPaymentConfiguration	
WorldPayInstallationID	*
Payment Gateway URL	https://select.wp3.rbsworldpay.com/wcc/purchase *
Currency	GBP (Pound Sterling) ▾ *

Service Disclaimer Content
We may collect and store the following personal information: physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

WorldPayBillingConfiguration			
Plan	Enable/Disable	Quota	Price
1	☐ Enable ☒ Disable	15 min(s) connection time quota with expiration	10.91
2	☐ Enable ☒ Disable	11 min(s) connection time quota	1
3	☐ Enable ☒ Disable	Valid until 12:00 the following day	5
4	☐ Enable ☒ Disable	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1
5	☐ Enable ☒ Disable		
6	☐ Enable ☒ Disable		
7	☐ Enable ☒ Disable		
8	☐ Enable ☒ Disable		
9	☐ Enable ☒ Disable		
10	☐ Enable ☒ Disable		

WorldPayNoteContent
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.

WorldPay Payment Configuration

WorldPayInstallation ID: The ID of the associated Merchant Account.

Payment Gateway URL: The default website of posting all transaction data.

Currency: The currency to be used for the payment transactions.

Service Disclaimer Content

View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

WorldPay Billing Configuration

These 10 plans are the plans in Billing Configuration, and the desired plan(s) can be enabled.

WorldPay Note Content

The message content will be displayed as a special notice to end customers.

Before setting up "WorldPay", it is required that the hotspot owners have a valid WorldPay "Merchant Account" from its official website: RBS WorldPay: Merchant Services & Payment Processing, going to rbsworldpay.com >> *support center* >> *account login*.

Step 1

-  Log in to the Merchant Interface.
-  Login url: www.rbsworldpay.com/support/index.php?page=login&c=WW
-  Select Business Gateway - Formerly WorldPay
-  Click [Merchant Interface](#)
-  Username: user2009
-  Password: user2009

Step 2

Select Installations from the left hand navigation

Step 3

Choose an installation and select the Integration Setup button for the specific environment.

Installation ID: 239xxx



223643 (Select Junior - 01server)		
232449 (Select Junior - Raja Dasgupta)		
237397 (Select Junior)		
237398 (Select Junior - Ivis Group)		
212370 (Select Junior - SA1 GLOBAL)		
213296 (Select Junior)		
214432 (Select Junior)		
215568 (Select Junior - Stof)		
215910 (Select Junior)		
219440 (Select Junior - Unearthed)		
239341 (Select Junior - futurepay)		
239805 (Select Junior - Neton)		
239 — (Select Junior - System)		
210071 (Select Junior - KNOG)		
210158 (Select Junior - Chris)		
222948 (Select Junior - innopacific)		

Step 4

Check Enable Payment Response checkbox.

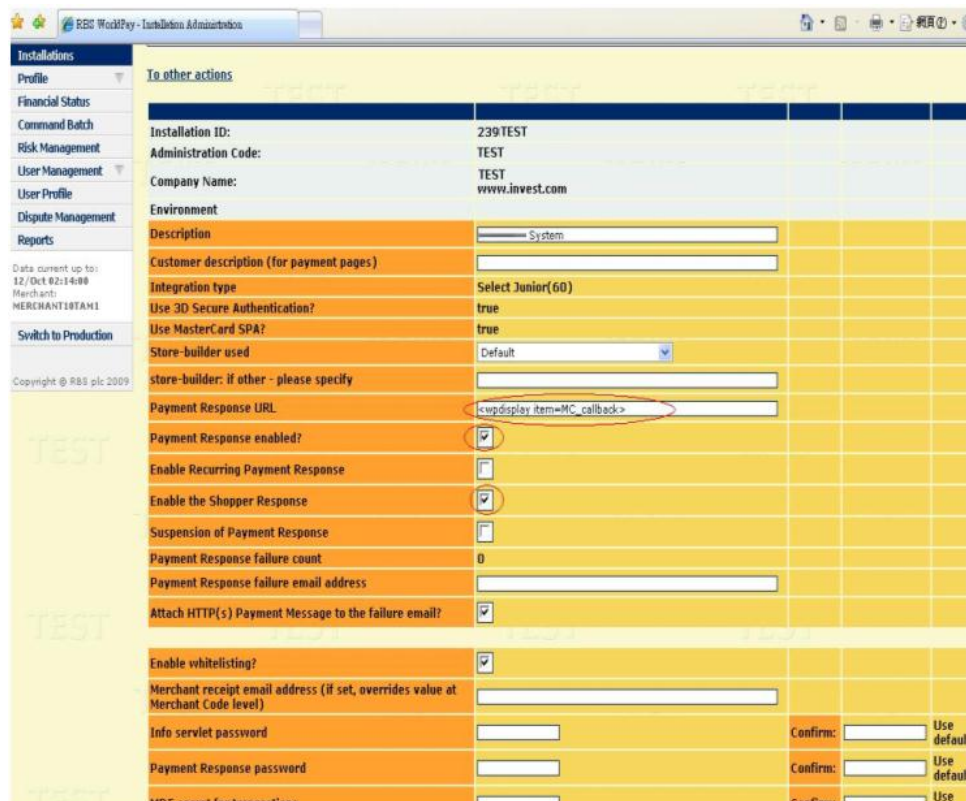
Step 5

Enter the Payment Response URL.

URL : <wpdisplay item=MC_callback>

Step 6

Check Enable the Shopper Response.



Step 7

Select the Save Changes button

Step 8

Input Installation ID and Payment Gateway URL in gateway UI.

-  Installation ID: 2009test
-  URL : <https://select.wp3.rbsworldpay.com/wcc/purchase>

External Payment Gateway	
☐ Authorize.Net	☐ PayPal
☐ SecurePay	☒ WorldPay
☐ Disable	

WorldPay Payment Page Configuration	
Installation ID	239--- *
Payment Gateway URL	https://select.wp3.rbsworldpay.com/wcc/purchase *
Currency	GBP (Pound Sterling) *

Note: The WAN IP of gateway must be a real IP.

Appendix F: Portal Page Customization

Since every Service Zone have their own configuration profiles and acts like a virtual gateway, administrators can customize or define their own portal pages utilized by users of that Service Zone.

The customizable pages of a Service Zone are: **Disclaimer Page**, **Login Page**, **Logout Page**, **Login Success Page**, **Login Fail Page**, **Logout Success Page**, **Logout Fail Page**, **Login Success Page for On-demand User**, **Port Location Mapping Free Login Page**, **Port Location Mapping Charge Login Page**.

Custom Pages	Disclaimer Page	Configure
	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Failed Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure
	Logout Failed Page	Configure

Main Menu >> System>Service Zone >> Service Zone Configuration

For each customizable page, the available customization options are to use: **Default Page**, **Template Page**, **Uploaded Page**, or **External Page**.

Login Page Selection for Users - Service Zone: Default	
☐ Default Page	☐ Template Page
☐ Uploaded Page	☒ External Page

Main Menu >> System >> Service Zone >> Service Zone Configuration >> Login Page

Default Page uses a web page stored within the system, its format and content cannot be changed.

Template Page also uses a web page stored within the system, but the contents such as text color, background color displayed text and logo can be configured according to your preferences.

Uploaded Page is to upload your self defined web page into the system, and use it as portal page displayed to the user.

External Page uses a web page stored in an external web server as the portal page for your users. Because the pages are located on a remote server, therefore special efforts are required by these external pages to parse, process and send necessary URL parameters to and from the system.

Since External Pages needs more attention and care to setup, its html codes also need to include mechanisms for processing the necessary URL parameters in order to work properly with the Access Controller, please refer to further details regarding on external pages in the following sections.

How External Pages Operate

Choose **External Page** if you desire to use an external web page for your custom pages. Simply enter the URL of your external webpage, click **Preview** button to check if it is reachable, take a look at how your external webpage will be displayed, then click **Apply** button.

Login Page Selection for Users - Service Zone: Default	
☐ Default Page	☐ Template Page
☐ Uploaded Page	☒ External Page

External Page Setting	
External URL	http://10.2.3.230/ExternalPage/login.html
Preview	

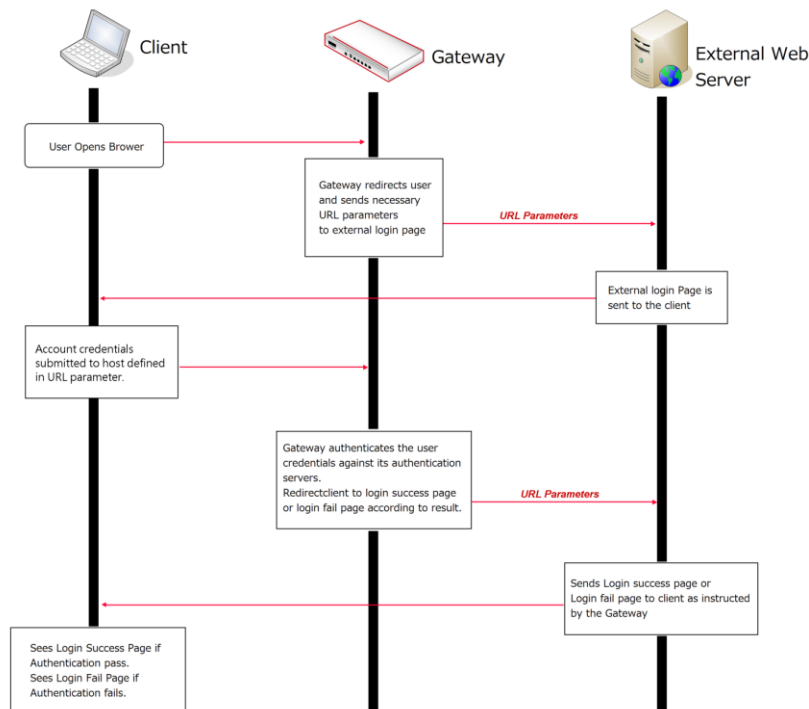
Apply
Cancel

Main Menu >> System >> Service Zone >> Service Zone Configuration >> Login Page

When a user connects to this Service Zone, opens a web browser and attempts to access the internet, the system will redirect the user to the external login page configured. Gateway while redirecting users to the external web page will also send URL parameters required for the operation, for instance user authentication. Therefore, each self-defined external pages (*Login*, *Logout*, *Login Success*, *Logout Success*, etc.) requires codes to handle **URL parameters** to and from the Gateway. A simple example is illustrated below for Login Page, please refer to **External Login Page Parameters** for URL parameter relating to other pages such as *Login Success Page* ... and etc.

Therefore it is important that your external pages are designed by someone with good knowledge of URL parameter utilization.

The diagram below explains how External Page operates using user login flow as illustration:



The URL parameters sent by the Gateway to the external login page are as follows:

Field	Value	Description
loginurl	String (URL encoded)	The URL which shall be submitted when user login.
remainingurl	String (URL encoded)	The URL which shall be submitted when user want to get remaining quota.
vlanid	Integer (1 ~ 4096)	VLAN ID
gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
umac	MAC format (separated by ':')	Client MAC address
session	String	Encrypted session information, include: client IP address, MAC address, date, and return URL.

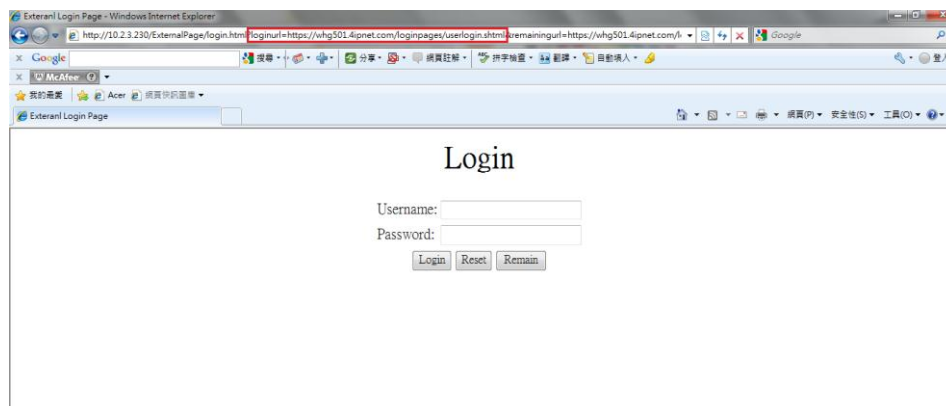
You will need to parse the required parameters in your html code. The following HTML code segment is an example of parsing *loginurl* parameter with a self define javascript function:

```
<FORM action="" method="post" name="form">
<script language="Javascript">
form.action = getVarFromURL(window.location.href, 'loginurl');
</script>
<INPUT type="text" name="myusername" size="25">
<INPUT type="password" name="mypassword" size="25">
<INPUT name="button_submit" type="submit" value="Enter">
<INPUT name="button_clear" type="button" value="Clear">
</FORM>
```

The following shows the corresponding self-defined javascript function used to parse the *loginurl* parameter:

```
function getVarFromURL(url, name) {
    if(name == "" || url == "") { return ""; }
    name = name.replace(/[\/|\\"|"]|.replace(/[\/|\\"|"]|"/g);
    var regObj = new RegExp("[\\?&]" + name + "=[^&#]*");
    var result = regObj.exec(url);
    if(result == null) { return ""; }
    else { return decodeURIComponent(result[1]); }
}
```

An external page example that the user will see upon launching a browser, highlighted in red you can see the URL parameters sent from the system:



URL Variables from Gateway

This section shows a list of URL variables of the external pages to be sent from the Gateway with its corresponding HTML coding.

External Login Page:

Variables:

Field	Value	Description
loginurl	String (URL encoded)	The URL which shall be submitted when user login.
remainingurl	String (URL encoded)	The URL which shall be submitted when user want to get remaining quota.
vlanid	Integer (1 ~ 4096)	VLAN ID
gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
umac	MAC format (separated by ':')	Client MAC address
Session	String	Encrypted session information, include: client IP address, MAC address, date, and return URL.

External Login Successful Page:

Variables:

Field	Value	Description
Uid	String	User ID (postfix is included)
Utype	String (LOCAL, RADIUS, ONDEMAND, POP3, LDAP, SIP, NT Domain)	Authentication server name
Umac	MAC format (separated by ':')	Client MAC address
sessionlength	Integer (Sec.)	RADIUS user session length (Only available for RADIUS user)
byteamount	Integer (Bytes)	RADIUS user volume limit (Only available for RADIUS user)
idletimeout	Integer (Sec.)	Idle timeout
acct-interim-interval	Integer (Sec.)	RADIUS accounting interim update interval (Only available for RADIUS user)
Logouturl	String (URL encoded)	The URL which shall be submitted when user want to logout.
Change_passwd_url	String (URL encoded)	The URL which shall be submitted when user want to change password. (Only available for LOCAL user)
ondemand_creation_url	String (URL encoded)	The URL which shall be submitted when user want to create on-demand user. (Only available for LOCAL user)
Vlanid	Integer (1~4096)	VLAN ID
Gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
Sz	Integer	Service Zone ID
Group	Integer	Group index
Policy	Integer	Policy index
max_uplink	Integer (b/s)	Maximum up-link rate

max_downlink	Integer (b/s)	Maximum down-link rate
req_uplink	Integer (b/s)	Minimum up-link rate
req_downlink	Integer (b/s)	Minimum down-link rate
next_page	String	Client redirection URL
CLASS	String	RADIUS CLASS attribute (Only available for RADIUS user)
WISPR-SESSION-TERMINATE-TIME	String, format: YYYY-MM-DDThh:mm:ssTZD	WISPr Session-Terminate-Time attribute (Only available for RADIUS user)
WISPR-SESSION-TERMINATE-END-OF-DAY	Integer (0/1)	WISPr Session-Terminate-End-Of-Day attribute, 0 or 1 to indicate termination rule. (Only available for RADIUS user)
WISPR-BILLING-CLASS-OF-SERVICE	String	WISPr Billing-Class-Of-Service attribute (Only available for RADIUS user)
WISPR-LOCATION-ID	String	WISPr Location-ID attribute (Only available for RADIUS user)
WISPR-LOCATION-NAME	String	WISPr Location-Name attribute (Only available for RADIUS user)
WISPR-BILLING-TIME	String, format: HH:MM	WISPr Billing-Time attribute (Only available for RADIUS user)
Session	String	Encrypted session information

External Error Page:

Variables:

Field	Value	Description
Msg	String, includes: The system is busy. Please try again later. Cannot find session related information. Please enable the Cookie in the browser setting or open a website to get a Cookie. Invalid IP address. Please check the IP address and try again. Invalid MAC address. Please check the MAC address and try again. Sorry, your account is not usable, because the authentication option is currently disabled. Please contact your network administrator. Sorry, your account is not usable, because the authentication option (associated with the postfix) is not found. Please contact your network administrator. Sorry, you are not allowed to log in, because your account is currently on the Black List. Sorry, you are not allowed to log in, because it is currently not the service	Error message

hour for your account.

You have already logged in.

Sorry, there is a system problem checking the information of your account (XXX).
Please contact your network administrator.

Invalid username or password.
Please check your username and password and try again.

Cannot identify the policy for your account.
Please contact your network administrator.

User of this device (the MAC address) is not allowed to use this account.
Please contact your network administrator.

Sorry, the external authentication server is currently unreachable.
Please contact your network administrator.

Sorry, you are not allowed to create a remote VPN connection.

Vlanid	Integer (1~4096)	VLAN ID
Gwip	IP format	Gateway activated IP address

External Logout Successful Page:

Variables:

Field	Value	Description
Uid	String	User ID (postfix is included)
Vlanid	Integer (1~4096)	VLAN ID
Gwip	IP format	Gateway activated IP address

External On-demand login successful page:

Variables:

Field	Value	Description
Uid	String	User ID (postfix is included)
Utype	String (LOCAL, RADIUS, ONDEMAND, POP3, LDAP, SIP, NT Domain)	Authentication server name
Umac	MAC format (separated by ':')	Client MAC address
sessionlength	Integer (Sec.)	On-demand user's quota of time type
byteamount	Integer (byte)	On-demand user's quota of volume type
idletimeout	Integer (Sec.)	Idle timeout
Logouturl	String (URL encoded)	Logout URL
redeemurl	String (URL encoded)	Redeem URL
Vlanid	Integer (1~4096)	VLAN ID
Gwip	IP format	Gateway activated WAN IP address

client_ip	IP format	Client IP address
Sz	Integer	Service Zone ID
Group	Integer	Group index
Policy	Integer	Policy index
next_page	String	Client redirection URL
max_uplink	Integer (b/s)	Maximum up-link rate
max_downlink	Integer (b/s)	Maximum down-link rate
req_uplink	Integer (b/s)	Minimum up-link rate
req_downlink	Integer (b/s)	Minimum down-link rate
Session	String	Encrypted session information

External Logout Fail Page:

Variables:

Field	Value	Description
Uid	String	User ID
Gwip	IP format	Gateway activated WAN IP address
Vlanid	Integer (1~4096)	VLAN ID

URL Variables to Gateway

This section shows a list of URL variables of the external pages to be sent to the Gateway with its corresponding HTML coding. **Path:** is the URL destination; **Input:** is the parameter required to be sent back; **Output:** is the feedback from the system.

User Login:

Path:

[\(LAN IP address or Internal Domain Name\) /loginpages/userlogin.shtml](#)

Input:

Field	Required	Value	Description
myusername	Required	String	User ID
mypassword	Required	String	User password
Session	Optional	String	Encoded string which contains some information of this session, default is taken from cookie.

Output:

No output, redirect user to login successful page.

User Logout:

Path:

[\(LAN IP address or Internal Domain Name\) /loginpages/logoff.shtml](#)

Input:

Field	Required	Value	Description
Uid	Optional	String	User ID, default is taken from cookie

Session	Optional	String	Encoded string which contains some information of this session, default is taken from cookie
---------	----------	--------	--

Output:

No output, redirect user to logout successful page.

Remaining quota (Credit balance):

Path:

(LAN IP address or Internal Domain Name) /loginpages/reminder.shtml

Input:

Field	Required	Value	Description
myusername	Required	String	User name
mypassword	Required	String	Password
ret_url	Optional	String (URL encoded)	Returned URL, default is pop_reminder.shtml
Command	Optional	String	getValue: If command is set to "getValue", the return URL would be ignored, and the page would only print out the available quota.

Output:

If command is set to "getValue", the output is simply "value".(secs. or bytes according to user type)

If command is not set and there is no ret_url is presented, client would be redirected to pop_reminder.shtml page, which shows remaining quota in our UI style. If ret_url is presented, client would be redirected to ret_url, and gateway would add these four variables in URL.

Field	Value	Description
Msg	String, including: Sorry, this feature is available for on-demand user only. Sorry, this username: XXX is not found. Sorry, this username: XXX is out of quota. Sorry, this username: XXX is expired. Sorry, this username: XXX is redeemed.	Error messages
Value	Integer (Sec. Or Byte) or error no. -1: Account not found. -2: Out of quota. -3: Expired. -4: Redeemed.	Remaining quota, if user is time type, the value is remaining seconds, if user is volume type, the value remaining bytes.
Uname	String	User name
Type	String, includes: TIME: Time type DATA: Volume type CUTOFF: Cut-off type	On-demand user billing type

Change password (Local User):

Path:

(LAN IP address or Internal Domain Name) /loginpages/user_change_password.shtml

Input:

Field	Required	Value	Description
Save	Required	1 (have to be 1)	
Opw	Required	String	Old password
Npw	Required	String	New password
Npwc	Required	String	Confirmed new password
ret_url	Required	String (URL encoded)	Return URL

Output:

Client would be redirected to ret_url and gateway would add result in ret_url which indicates the result of changing password.

Field	Value	Description
Result	String, including: Change password successfully User password is incorrect Invalid password format	Result and error messages

Redeem (On-demand user):

Path:

(LAN IP address or Internal Domain Name)/loginpages/redeemuserlogin.shtml

Input:

Field	Required	Value	Description
Uid	Optional	String	Current user ID (If not presented, user name stored in cookie is the default value)
upassword	Optional	String	Current user password (If not presented, password stored in cookie is the default value)
myusername	Required	String	Redeem user ID
mypassword	Required	String	Redeem user password
ret_url	Optional	String (URL encoded)	Return URL, login successful page is the default value

Output:

If no ret_url is presented, client would be redirected to login successful page, and in addition, a JavaScript window would pop-up and show the result. If ret_url is presented, client would be redirected to ret_url and gateway would add an additional variable rmsg to indicate redeem procedure result.

Field	Value	Description
rmsg	String, including: Redeem process completed. Original user name can not be found from the database. Redeem user name can not be found	Result and error messages

from the database.

Original user password is incorrect.

Redeem user password is incorrect.

Original user type and ondemand user type do not match.

Original user has not login.

Redeem user login already.

Had been redeemed before.

User run out of quota.

Maximum allowable time is exceeded.

Maximum allowable memory space is exceeded.

Wrong postfix please check it.

This account is expired.

On-demand account creation (Local User)

Path:

(LAN IP address or Internal Domain Name) /loginpages/UserAuthentication/OnDemandRecept.shtml

Input:

Field	Required	Value	Description
buttonNo	Required	Integer (1~10)	Billing Plan No.
random	Optional	Integer	A random number, this number is to prevent quick-click issue in IE 6.0.
ret_url	Optional	String (URL encoded)	Return URL.

Output:

If no ret_url is presented, the client would be redirected to a ticket page in our UI style. If ret_url is presented, client would be redirected to ret_url and receive the result containing created on-demand account information.

Field	Value	Description
Result	String, the format is: (separated by ',') username, password, expiretime, usage, price, duration, serial number	If ret_url is presented, the client would be redirected to ret_url page and carry the result valuable. expiretime is account expiration time which is a Linux time stamp, and duration is account duration time and the unit is 'day', serial number is account s/n.